Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Promoting the Deployment of 5G Open Radio	)	GN Docket No. 21-63
Access Networks	)	

COMMENTS OF MAVENIR SYSTEMS, INC.

Mavenir Systems, Inc.

Caressa D. Bennet
E. Alex Espinoza
Womble Bond Dickinson (US) LLP
1200 19th Street, N.W.
Suite 500
Washington, D.C. 20036
(202) 467-6900

Counsel for Mavenir Systems, Inc.

Table of Contents

SUMMARY

Mavenir fully supports the Commission in its efforts to aid U.S. wireless operators and ecosystem suppliers to develop, deploy, and employ Open RAN architecture in U.S. wireless networks. Networks built with open and interoperable interfaces are no different from networks with proprietary interfaces, with the main exception that the interfaces are published, *open and interoperable*. Open RAN is not a technology; it refers to open and interoperable interfaces used within existing technology. The current state of U.S. RAN is one of perpetuating proprietary networks that continues to lock out U.S. suppliers. To truly *open the RAN* to all vendors and new innovative solutions, and truly level the playing field, the Commission must take quick and decisive action, including: *explicitly prioritizing Open RAN architecture; adopting preferences for U.S. vendors; and incentivizing U.S. wireless operators to prefer U.S. suppliers*.

As it weighs the record being gathered through this NOI, the Commission should take into consideration the following:

- Open RAN is not a technology—it is open and interoperable interfaces.
- U.S. suppliers face the real risk of being locked out of both the global and U.S. RAN markets.
- The U.S. RAN market is effectively a duopoly, and current policies perpetuate foreign-owned incumbents' proprietary systems.
- Allied nations are making significant investments in Open RAN, and some are preferencing local suppliers.
- Encouraging Open RAN deployment in the FCC's Supply Chain Reimbursement Program.
- Supporting increased U.S. participation in 3GPP to promote the advancement of open and interoperable interfaces.
- Open RAN is ready today, and is being deployed around the world.

Open RAN is currently being planned to be used at scale internationally with our allied nations, *e.g.*, the United Kingdom, Germany, India, France, and Japan, among others, who are significantly investing in OpenRAN, and in some cases preferencing local vendors to build secure, cost effective next generation networks. Those investments and preferences shift the ultimate risks onto U.S. suppliers, who could consequently be locked out of those international markets, in addition to being currently locked out of the U.S. RAN market.

The Commission must encourage U.S. operators and their foreign incumbent suppliers to support the deployment of Open RAN domestically. The Commission should also actively promote domestic participants in 3GPP, both financially, and via the Commission's statutory authority because today foreign-owned incumbents control the primary international standard setting body, 3GPP.

Furthermore, unless the Commission takes action now, U.S. vendors will be locked out of the RAN market for approximately ten years until the arrival of 6G, and will lose the opportunity that the FCC's Reimbursement Program presents. Open RAN is *the* cost effective and secure solution to diversify the U.S. communications supply chain. Open RAN allows multiple vendors to provide equipment or services; enabling vendors to compete to provide those services and equipment in the process. Open RAN's zero trust philosophy—never trust, always verify—makes it inherently more secure than proprietary RAN solutions. Open RAN's specifications provide wireless operators transparency; allowing the visibility to target equipment to upgrade, repair, and/or provide an overarching security assessment.

Moreover, not only does the Commission have the policy imperative to uphold its competitive market principles, and thereby open interfaces and require interoperability, it has the legal authority to do so under Title III, CALEA; sections 201(b) and 254 of the Communications Act; and section 706 of the 1996 Act.

Accordingly, to secure our networks, and ensure American leadership in 5G, the Commission should immediately proceed to a Notice of Proposed Rulemaking to open the RAN to Open RAN.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Promoting the Deployment of 5G Open Radio Access Networks	))	GN Docket No. 21-63

COMMENTS OF MAVENIR SYSTEMS, INC.

Mavenir Systems, Inc. ("Mavenir"), through its undersigned counsel, respectively submits its comments in response to the Notice of Inquiry in the above-captioned proceeding.[1] Mavenir commends the Federal Communications Commission ("Commission") for undertaking this long overdue inquiry into the state of the Radio Access Network ("RAN") by recognizing the need to break the stranglehold that two foreign-owned incumbents now have on the U.S. RAN market simply by fostering the adoption of open and interoperable interfaces ("Open RAN") to allow the provision of RAN equipment and services by multiple competing vendors. As discussed below, prompt action by the Commission to remove barriers to the implementation of Open RAN and facilitate its deployment, will have overwhelming benefits for the wireless ecosystem through the introduction of competition in the current duopoly market, reductions in cost, increases in efficiency, and significant enhancements to the security of U.S. wireless networks against malicious foreign and domestic actors. Following the NOI, Mavenir urges the Commission to initiate a Notice of Proposed Rulemaking to consider adoption of specific proposals to further the implementation of Open RAN.

[1] *Promoting the Development of 5G Open Radio Access Networks*, GN Docket No. 21-63, Notice of Inquiry, FCC 21-31 (Mar. 18, 2021) (Open RAN NOI).

I. The Present State of Open RAN and its Standards

The U.S. RAN market is now dominated by two foreign-owned incumbents – Ericsson and Nokia. These two companies, along with Huawei and ZTE, took control over RAN standards-setting bodies such as 3GPP. Fortunately, other standards organizations were formed to counter this domination. To date, the best alternatives to proprietary 3GPP-defined RAN interfaces and protocols is Open RAN, which is based on 3GPP and O-RAN Alliance specifications that use open interfaces and allow for interoperability.

A. Current Ecosystem

With respect to the current state of the Open RAN ecosystem,[2] before the U.S. government's efforts to eliminate, what the U.S. determined to be, untrusted vendors from U.S. telecommunications networks, the U.S. mobile network supply chain was dominated by four foreign headquartered companies: Huawei, ZTE, Ericsson, and Nokia. In a memorandum preceding an April 2021 House Energy and Commerce Subcommittee on Communications and Technology hearing,[3] Committee Chairman Rep. Frank Pallone recognized that the status quo is such that "[w]hen a network . . . needs to be upgraded or modified, a wireless operator must either purchase equipment from the same manufacturer or replace most of the network equipment with that of another manufacturer."[4] During that same hearing, a witness for Rakuten Mobile, a mobile network operator and technology company that has deployed its network to Open RAN principles, testified that the wireless market has historically been one reliant upon

[2] Open RAN NOI, at 11, para. 55.

[3] *See generally Leading the Wireless Future: Securing American Network Technology*: Hearing before the Subcomm. on Commc'ns & Tech. of the H. Comm. on Energy & Commerce, 117th Cong. (2021).

[4] Memorandum from Committee on Energy & Commerce Staff to Subcommittee on Communications & Technology Members and Staff (Apr. 19, 2021), https://docs.house.gov/meetings/IF/IF16/20210421/112475/HHRG-117-IF16-20210421-SD003.pdf.

vertical solutions from a few vendors: "It has always been about replacing proprietary hardware with new proprietary hardware—it was never about software. While that model has evolved somewhat from its early days, the reality is that there are now only a handful of mobile network vendors."[5] Indeed, with the effective ban of Huawei and ZTE, the U.S. RAN market is left with essentially two foreign-owned incumbents, leaving a duopoly with unprecedented control over pricing, innovation, and competitive entry. This duopoly continues to provide proprietary end-to-end RAN solutions, which have the effect of blocking competitive vendors from equipping or servicing wireless networks. The Commission can end this dominance over the RAN market and expand the domestic supply chain for RAN equipment and services by incentivizing wireless operators to begin to incorporate Open RAN principles into their wireless networks. As discussed below, Open RAN is not a technology, it is based on principles of open and interoperable interfaces that resets policy for wireless standards organizations.

With respect to the Commission's question seeking comment on companies "offering baseband hardware, network virtualization, packet core functionality, or other network components,"[6] Mavenir is the industry's only end-to-end cloud-native network software provider. The company provides access and edge solutions and serves as an integrator for virtualized networks including those built on Open RAN principles. Though Mavenir is predominantly a software-based innovator, it is working to manufacture remote radio heads for

[5] *Leading the Wireless Future: Securing American Network Technology*: Hearing before the Subcomm. on Commc'ns & Tech. of the H. Comm. on Energy & Commerce, 117th Cong. (2021) (testimony of Testimony of Tareq Amin, Representative Director, Executive Vice President and CTO, Rakuten Mobile), https://www.congress.gov/117/meeting/house/112475/witnesses/HHRG-117-IF16-Wstate-AminT-20210421-U1.pdf

[6] Open RAN NOI at 11, para. 25. "Baseband" is a reference to "the original frequency range of a transmission signal before it is modulated, with the "baseband unit" (BBU) as the equipment that processes baseband in telecommunications systems. For high-level description of the BBU and other components of a typical wireless telecom station, see EXFO, *Baseband Unit*, https://www.exfo.com/en/resources/glossary/baseband-unit/ (last visited Apr. 16, 2021).

the U.S. supply chain, replacing products that are all currently manufactured in China to help lower costs for deployment, and build up this manufacturing capability in the U.S. Addressing the Commission's query,[7] companies that offer baseband hardware include Intel, Dell, AMD, Nvidia, Kontron, HP, and Quanta. Companies offering network virtualization include VMware, Mavenir, Altiostar, Red Hat, Wind River, Amdocs, Nokia, Ericsson, Cisco, and Adva. Companies that offer packet core functionality include Mavenir, Affirmed (Microsoft), Cisco, NEC, and Samsung.

B. Current State of Standards and Foreign-Owned Incumbent Control Over Standards-Setting Bodies

The Commission seeks comment on the "current state of standards and specifications for 5G and Open RAN."[8] Currently, there are two main international standard-setting bodies for RAN mobile technology: 3GPP[9] and the O-RAN Alliance. 3GPP sets global specifications for mobile networks. The organization is driven by the major equipment vendors. This has allowed certain companies like Huawei, Ericsson, and Nokia to maintain control over the mobile infrastructure market with their proprietary equipment, limiting new suppliers from entering the market. Not surprisingly, to date, 3GPP has not adopted open and/or interoperable interfaces and front haul protocols for the RAN. This has resulted in 3GPP RAN specifications that are proprietary and cannot be made interoperable.

There are hundreds of parameters necessary for interoperable interfaces that are missing from 3GPP specifications, and in Mavenir's observation, there is little interest within 3GPP in

[7] Open RAN NOI at 11, para. 25.

[8] *Id*. at 10, para. 24.

[9] *See About 3GPP Home*, https://www.3gpp.org/about-3gpp/about-3gpp (last visited Apr. 13, 2021) ("The 3rd Generation Partnership Project (3GPP) unites [Seven] telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), known as 'Organizational Partners' and provides their members with a stable environment to produce the Reports and Specifications that define 3GPP technologies. The project covers cellular telecommunications technologies, including radio access, core network and service capabilities, which provide a complete system description for mobile telecommunications.").

working to open and interoperate those RAN specifications. This was made clear in the adoption of 5G specifications, where spectrum saving features were made vendor-specific, including for example, interwork between 4G and 5G for Non-Standalone architecture, carrier aggregation, Coordinated MultiPoint (CoMP), enhanced Inter-cell Interference Coordination (eICIC), and PIM Cancellation.[10] Of particular concern, the solutions from Nokia, Ericsson, and Huawei are *not even interoperable amongst themselves nor can they be overbuilt in the same region, forcing operators' continued dependency on a single supplier*.

As noted, large foreign suppliers are driving standard-setting efforts within 3GPP. Participation in 3GPP is extremely costly, as are the travel costs associated with participation, which translates to smaller players being left out because they do not have the resources to meaningfully participate. This participation cost has further solidified the dominance of the large, foreign-owned suppliers, within 3GPP who have the resources to send large numbers of representatives to every meeting and thus dominate the 3GPP's work. Representatives of these suppliers also chair a number of 3GPP working groups, further enabling these vendors to keep interfaces proprietary and competitors at bay.

These actions by large foreign-owned suppliers, effectively shut out smaller suppliers and newer entrants from the RAN market. The larger foreign-owned suppliers, do not support open and interoperable interfaces, presumably because they recognize it as a threat to their market share; they control 3GPP by writing the rules for global telecommunications networks and protecting their proprietary networks and market share. The game is stacked in their favor, and Mavenir's view is that they write the rules against smaller suppliers and newer entrants, blocking them from meaningfully contributing to 3GPP and competing in the lucrative RAN marketplace.

[10] *See* Mobile Experts, Open RAN: Good and Getting Better (2020) *in* Mavenir, Your Guide to OpenRAN 106 (2021) (Mavenir e-book attached).

To fill the void in 3GPP standards and to help support open and interoperable specifications, the O-RAN Alliance was founded. Today, the O-RAN Alliance is led by 28 operators with 240 suppliers participating.[11] The O-RAN Alliance has helped to advance Open RAN architectures and is defining the interface specifications that were left as frameworks in 3GPP next generation RAN solutions, which are open, intelligent, virtualized and fully interoperable. O-RAN specifications have helped move the greater RAN ecosystem forward, but its specifications have not been adopted by 3GPP, which remains the primary RAN global standard-setting organization.

To advance open and interoperable standards and to promote competition, the Commission should actively encourage and provide support for more U.S. companies to participate in 3GPP. One recent study reports that within 3GPP, "Huawei was the biggest contributor to 5G standards," leading in "overall contributions to the end-to-end 5G standards."[12] The Commission's recent work in the *Supply Chain Proceeding*[13] would be significantly undermined if banned companies[14] remained free to control 5G standards. To increase U.S.

[11] Mavenir is a member of the O-RAN Alliance. For a list of members, see O-RAN Alliance, *Membership*, https://www.o-ran.org/membership (last visited Apr. 16, 2021).

[12] Mike Dano, *Study: Huawei was the biggest contributor to 5G standards*, Light Reading (Mar. 17, 2020), https://www.lightreading.com/5g/study-huawei-was-the-biggest-contributor-to-5g-standards/d/d-id/758279 (citing Strategy Analytics Study, "Who Are the Leading Players in 5G Standardization? An Assessment for 3GPP 5G Activities")

[13] *E.g. Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs,* Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd 11423 (2019) (*Supply Chain First Report and Order*); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs,* Second Report and Order, 35 FCC Rcd 14284 (2020) (*Supply Chain Second Report and Order*). For the sake of brevity, we refer to these two orders as the *Supply Chain Proceeding*.

[14] *Public Safety and Homeland Security Bureau Announces Publication of the List of Equipment and Services Covered by Section 2 of the Secure Networks Act*, WC Docket No. 18-89, Public Notice, DA 21-309 (PSHSB 2021). *See also generally, e.g., Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation*, Memorandum Opinion and Order, 35 FCC Rcd 14435 (2020) (denying Huawei's Application for Review of Commission's Final Designation Order); Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – ZTE Designation, Memorandum Opinion and Order, 35 FCC Rcd 13146 (PSHSB 2020) (Denying ZTE's Petition for Reconsideration of the Commission's final designation of ZTE).

participation, the Commission should actively promote domestic suppliers in 3GPP by encouraging Congress to financially support those suppliers' involvement in 3GPP.[15]

The USA Telecommunications Act of 2020 establishes a role for the Commission to advise NTIA in administering the Public Wireless Supply Chain Innovation Fund, which is charged with promoting and deploying "open interface wireless access networks."[16] The Commission can take full advantage of this role, and harness its in-house technical experts—as well as those from the private sector, via, *e.g.*, the Communications Security, Reliability, and Interoperability Council (CSRIC)—to participate and help advance open and interoperable interfaces, which will support more competition and a supply chain that includes U.S. suppliers. Without more U.S. companies at the table, the market will be left with the continued perpetuation of a few foreign-headquartered companies dominating the global RAN supply chain with proprietary solutions, and the risk that U.S. companies will be eliminated from competing in this market.

C. eCPRI is Not an Alternative to Open RAN

The Commission asks about other alternatives to Open RAN, such as eCPRI.[17] As it standard currently stands, eCPRI is not an alternative to Open RAN, and its adoption will neither

[15] Mavenir notes that a bipartisan group of U.S. Senators recently asked President Biden to include $3 billion to fund the Utilizing Strategic Allied Telecommunications Act of 2020 (USA Telecommunications Act) in the Presidents FY 2022 budget request. The USA Telecommunications Act contains two separate funds, which would "enable the development and deployment of an Open RAN approach to network standardization for nationwide 5G (and successor) wireless capabilities." Letter from Sen. Mark Warner et al., Chairman, Senate Select Committee on Intelligence, to Pres. Joseph R. Biden, Jr. (Apr. 6, 2021), https://www.warner.senate.gov/public/_cache/files/1/d/1df21e57-94af-461b-a42a-6cd783585fb1/E823553A6FAE8062B60F9EA6C25BB4D5.biden-ssci-6apr21.pdf

[16] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, §9202, 134 Stat 3388, 4788-89.

[17] *See* Open RAN NOI at 11, para. 24. CPRI (Common Public Radio Interface), is an "Internal interface specification for radio base stations. CPRI is also the industry association regulating the specification." Anil Umesh et al., *Overview of O-RAN Fronthaul Specifications*, 21 NTT DOCOMO Tech. J. 1, 47 n.4 (2019), https://www.nttdocomo.co.jp/english/binary/pdf/corporate/technology/rd/technical_journal/bn/vol21_1/vol21_1_en_total.pdf. eCPRI is the "Internal interface for radio base stations prescribed by CPRI, an industry association." *Id.*

break the stranglehold that the dominant foreign-owned vendors have on end-to-end RAN solutions, nor facilitate entry of vendors of RAN components.

At a high level, there are two eCPRI solutions: (1) a 3GPP eCPRI proprietary solution—for which only the framework has been published; and (2) the O-RAN eCPRI, which is fully specified, and is now being adopted by the Open RAN community.

The 3GPP eCPRI specifications are not complete interfaces, and competitive vendors have been shut out from the promulgation of that standard. In addition, Nokia, Ericsson, Huawei, and NEC produced the standard outside of 3GPP to include even more proprietary functions to the benefit of those four foreign companies, and to the exclusion of competitors.[18] Unfortunately, 3GPP eCPRI is either missing hundreds of parameters, or those parameters are treated as proprietary, and thus cannot be considered an Open RAN alternative.

The O-RAN Alliance's first task was to develop a complete O-RAN eCPRI solution in order to open up the interfaces for the Control, User, and Management specifications, which are critical to fronthaul[19] operations so that they could be fully interoperable. While there have been

at n.8. Ericsson, Huawei, NEC, and Nokia explain that "The Common Public Radio Interface (CPRI) is an industry cooperation aimed at defining publicly available specifications for the key internal interface of radio base stations, such as eCPRI connecting the eCPRI Radio Equipment Control (eREC) and the eCPRI Radio Equipment (eRE) via a so-called fronthaul transport network." Ericsson AB, Huawei Technologies Co, Ltd, NEC Corporation, and Nokia, Common Public Radio Interface: eCPRI Interface Specification V2.0 at 4 (2019), http://www.cpri.info/downloads/eCPRI_v_2.0_2019_05_10c.pdf.

[18] The eCPRI specification outlines that "The parties cooperating to define the [eCPRI] specification are *Ericsson AB, Huawei Technologies Co. Ltd, NEC Corporation and Nokia.*" Ericsson AB, Huawei Technologies Co, Ltd, NEC Corporation, and Nokia, Common Public Radio Interface: eCPRI Interface Specification V2.0 at 4 (2019), http://www.cpri.info/downloads/eCPRI_v_2.0_2019_05_10c.pdf (emphasis added).

[19] Fronthaul is the "Circuit between the baseband processing section in base station equipment and radio equipment using optical fiber." Anil Umesh et al., *Overview of O-RAN Fronthaul Specifications*, 21 NTT DOCOMO Tech. J. 1, 46 n.3 (2019), https://www.nttdocomo.co.jp/english/binary/pdf/corporate/technology/rd/technical_journal/bn/vol21_1/vol21_1_en_total.pdf.

cases where, for example, two foreign suppliers, namely Nokia and Samsung[20] have shared and created a separate specification to show interoperability, this was still developed within a proprietary system, resulting in the protection of those suppliers' market share. Unfortunately, while the Open Radio Interface (ORI) CPRI specification[21] was fully developed, it was never adopted as "*the*" standard for RAN fronthaul and is not suitable for 5G requirements. Once again, proprietary standards were adopted and continue to be used by the large foreign-owned vendors.[22]

II. Open RAN is Deployment-Ready and In Use Now

The Commission can and should open U.S. networks to Open RAN and break the foreign-owned incumbents' domination. Open RAN is ready now and is currently being deployed domestically and internationally to great acclaim. Open RAN offers significant benefits that will tailor networks to the needs of network operators, both large and small. Moreover, an Open RAN network is no more difficult to build and operate than a proprietary

[20] *See Ecosystem Building: Samsung and Nokia Work Together to Conduct 5G Interoperability Testing*, Samsung (Feb. 24, 2017), https://www.samsung.com/global/business/networks/insights/blog/ecosystem-building-samsung-and-nokia-work-together-to-conduct-5g-interoperability-testing/.

[21] "In general mobile radio base stations consist of a BaseBand Unit (BBU) and a Radio Frequency Unit (RFU), which usually is a Remote Radio Head (RRH) in a distributed base station architecture. In order to gain flexibility operators are looking for distributed base station architectures with separate BBUs and RRHs. In order to gain interoperability, BBU and RRH are interconnected via an open BBU-RRH Interface (ORI) for flexible combination from different vendors. ORI is about a digitized radio base station interface that establishes a connection between "Radio Equipment Control" (REC) and "Radio Equipment" (RE) enabling single-hop and multi-hop topologies. Different information flows (User Plane data, Control and Management Plane data, and Synchronization Plane data) are multiplexed over the interface. ORI [Open Radio equipment Interface] covers OSI protocol layer 1, Layer 2 up to Layer 7." European Telecommunications Standards Institute (ETSI), ETSI GS ORI 001 V4.1.1 - Open Radio equipment Interface (ORI); Requirements for Open Radio equipment Interface (ORI) (Release 4) at 4-5 (2014), https://www.etsi.org/deliver/etsi_gs/ORI/001_099/001/04.01.01_60/gs_ORI001v040101p.pdf

[22] *See* Iain Morris, *Open Conflict Over Open RAN*, Light Reading (Feb. 14, 2019), https://www.lightreading.com/mobile/fronthaul-c-ran/open-conflict-over-open-ran/d/d-id/749437?page_number=3 (last visited Apr. 16, 2021).

RAN network, and there are significant upsides from the improved cost savings, security, and resiliency that Open RAN presents.

A. Open RAN Domestic Deployments

Domestically, Mavenir is working with DISH to deploy the first and largest standalone 5G Open RAN network in the U.S., which will launch in Las Vegas by the end of September and "is expecting to cover 20 percent of the U.S. population by June 2022, and 70 percent by June 2023."[23] Domestically overall, however, other wireless operators are currently vendor-locked and are dependent on two foreign-owned incumbent suppliers to service their existing networks. U.S. wireless operators have shown an interest in Open RAN[24]—and several have joined the Open RAN Policy Coalition to help advance policies to support deployment[25]—but apart from DISH, have not yet gone as far as operators in Europe to deploy Open RAN. In Europe five major operators have signed onto a Memorandum of Understanding, committing to deploy Open RAN throughout the European continent's networks.[26]

To encourage timely and secure domestic deployments, the Commission should explicitly prioritize Open RAN, encourage competition, adopt preferences for U.S. companies, and

[23] Press Release, Mavenir, Dish Selects Mavenir to Deliver Cloud-Native Open RAN Software for Nation's First Virtual 5G Wireless Broadband Network (April 23, 2020), https://mavenir.com/press-releases/dish-selects-mavenir-to-deliver-cloud-native-Open RAN-software/

[24] Verizon, for example, is now deploying Samsung's vRAN (virtualized RAN) in "parts of upstate New York and New England," Bevin Fletcher, *Verizon deploys Samsung vRAN in 5G expansion*, Fierce Wireless (Jan. 22, 2021 1:22pm), https://www.fiercewireless.com/5g/verizon-deploys-vran-from-samsung-for-5g-expansion. Verizon is also reported to be employing Open RAN equipment "to construct a 5G network in its millimeter wave (mmWave) and C-band spectrum holdings." Mike Dano, *Verizon to start deploying open RAN gear this year*, Light Reading (Mar. 11, 2021), https://www.lightreading.com/open-ran/verizon-to-start-deploying-open-ran-gear-this-year/d/d-id/768021#:~:text=Koeppe%20added%20that%20Verizon%20will,hardware%20vendors%20into%20its%20network.

[25] *See* Open RAN Policy Coalition, https://www.openranpolicy.org/about-us/members/ (last visited Apr. 22, 2021). Sixty companies have joined together as the Open RAN Policy Coalition, through which they advocate for government policies—in the U.S. and abroad—that support the development and adoption of open and interoperable Open RAN interfaces. Mavenir is a member of the coalition and serves on its Board of Directors.

[26] *See generally* Open RAN NOI at 13, para. 29 (seeking comment on Vodafone Group Plc, Telefonica S.A., Deutsche Telekom AG, and Orange S.A.'s signing a "Memorandum of Understanding signaling their commitment to deploy Open RAN solutions across Europe.").

incentivize wireless operators to consider cost when receiving federal support for their networks. International efforts like the European Memorandum of Understanding (the "European Open RAN MOU") have grave implications for U.S. leadership in this area. From a leadership perspective, the U.S. is falling behind. Allied nations are moving ahead with their next generation networks based on Open RAN, providing tax incentives and funding assistance, and some countries are even implementing domestic preferencing for their vendors. Without positive U.S. government involvement along with Commission action to dislodge foreign control over equipment manufacturing, proprietary standards, and standards-setting bodies, U.S. suppliers risk being shut out of the 5G RAN market domestically and internationally.

There are no unique challenges in "U.S. wireless network industry, spectrum policies or geographical or other factors that present unique challenges to [domestic] Open RAN deployment,"[27] that do not exist for proprietary network deployments. Rather it is the fundamental issue of a proprietary standard setting process combined with proprietary equipment, protocols, and interfaces that prevent competitors from competing on a level playing field with the two foreign-owned incumbent suppliers today.

The bottom line is that today, *there is no U.S. wireless RAN network industry*: The U.S. has ceded domestic manufacturing and is now entirely dependent on two foreign-owned incumbents. These foreign-owned incumbents now control the U.S. supply chain, policy and advocacy-focused trade associations, and international standard setting organizations—which are not being influenced in any way by U.S. headquartered vendors or the U.S. government. Writing to President Biden, a group of 18 former military and intelligence community heads warn that "[c]ontinuing the current [5G] leadership vacuum will only embolden our competitors, leaving

[27] Open RAN NOI at 14, para. 30.

our allies vulnerable to untrusted equipment and threatening the security of allied intelligence sharing."[28]

B. Open RAN International Deployments

International developments in Open RAN offer great lessons for the Commission.[29] From Europe to Asia, U.S. allies are building Open RAN and are incorporating "domestic preferencing" of suppliers located within their country or continent. Specifically:

- The Government of France is supporting French suppliers in its efforts to reduce its dependency on Huawei.[30]
- The German government is primarily backing German and European suppliers for a similarly-focused effort earmarking over €300 million—$359 million USD—for Open RAN technology.[31]
- The United Kingdom announced its *5G Supply Chain Diversification Strategy*[32] to help diversify and grow its mobile supply chain, in part through multi-million investment in 5G projects, [33] and has announced a $350 million project to develop Open RAN systems

[28] Letter from Gen. Keith Alexander et al., Former Director, National Security Agency, to Pres. Joseph R. Biden (Apr. 13, 2021), *available at* https://www.semiconductors.org/wp-content/uploads/2021/04/2021.04.13-National-Security-Letter.pdf.

[29] *See generally* Open RAN NOI at 14, para. 30 (seeking comment on successful deployments and international efforts).

[30] *See, e.g.*, *Sequans Receives Major Funding Award for 5G Development from the French Government*, Nasdaq.com, (Jan. 28, 2021 8:00AM EST), https://www.nasdaq.com/press-release/sequans-receives-major-funding-award-for-5g-development-from-french-government-2021 (last visited Apr. 14, 2021); Helene Fouquet et al., *France's Huawei Ban Begins to Kick In With Purge in Urban Areas*, Bloomberg, (Mar. 1, 2021, 6:40AM), https://www.bloomberg.com/news/articles/2021-03-01/france-s-huawei-ban-begins-to-kick-in-with-purge-in-urban-areas (last visited Apr. 12, 2021).

[31] Laurens Cerulus, *Berlin's €2B plan to wean off Huawei (and Nokia and Ericsson too)*, Politico (Feb. 2, 2021, 7:26pm), https://www.politico.eu/article/germany-huawei-telecoms-plan/ (last visited Apr. 14, 2021).

[32] *See* Government of the United Kingdom, Department for Digital, Culture, Media & Sport, *5G Supply Chain Diversification Strategy*, (December 7, 2020), https://www.gov.uk/government/publications/5g-supply-chain-diversification-strategy/5g-supply-chain-diversification-strategy (last visited Apr. 15, 2021) (stating in part the UK is "Launching a major Open RAN trial in the UK to speed up the development of Open RAN and laying foundations for roll out in UK networks").

[33] *See* Ray Le Maistre, Open RAN architectures at heart of UK 5G projects, TelecomTV (Jan. 18, 2021), https://www.telecomtv.com/content/open-ran/open-ran-architectures-at-heart-of-uk-5g-projects-40645/ (last visited Apr. 15, 2021).

and equipment.[34] The Livingston diversity report, discussed further below, recommends making 25% of the UK market available to new and small suppliers by 2025.[35]

- The Indian government is expected to preference Indian suppliers as it builds out its next generation networks.[36]
- Japan has announced a number of tax incentives for products built through open and interoperable interfaces,[37] effectively eliminating participation in their networks by certain proprietary equipment manufacturers. Japan and the U.S. have agreed to support Open RAN together, "by fostering innovation and by promoting trustworthy vendors and diverse markets."[38]

If the U.S. government does not similarly support U.S. suppliers with funding, incentives, and preferences, we face the unfortunate reality that U.S. government funds—used to purchase equipment with proprietary interfaces manufactured by foreign-headquartered companies—will effectively be used to shut out U.S. suppliers.

Through these international deployments, we have learned that Open RAN-based networks are more cost efficient to construct and maintain—making them more advantageous for underserved communities, including low-income and rural environments. Aside from the cost efficiencies—nearly 40% in capital expenditure (CapEx) and 34% in operating expenditure

[34] Thomas Duesterberg, *U.S. Efforts To Counter Huawei 5G Dominance Making Progress: Open RAN Playing Growing Role*, Forbes (Mar 17, 2021, 11:33 AM), https://www.forbes.com/sites/thomasduesterberg/2021/03/17/us-efforts-to-counter-huawei-5g-dominance-making-progress-open-ran-playing-growing-role/?sh=3eb83f91655e (last visited Apr. 15, 2021).

[35] *See* Telecoms Diversification Taskforce, Findings and Report 12-13, 15 (2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975007/April_2021_Telecoms_Diversification_Taskforce_Findings_and_Report_v2.pdf. *See also* section II.I below.

[36] Kiran Rathee, *TRAI Chairman: 'Open RAN will Present Opportunities*, The Indian Express (Jan. 20, 2021 6:04:53 am), https://indianexpress.com/article/business/trai-chairman-open-ran-will-present-opportunities-7153590/ (last visited Apr. 15, 2021).

[37] Mihoko Matsubara, *Japan's 5G Approach Sets a Model for Global Cooperation*, LawFare (Sept. 14, 2020, 9:12 AM), https://www.lawfareblog.com/japans-5g-approach-sets-model-global-cooperation (last visited Apr. 15, 2021).

[38] White House, *Fact Sheet: U.S.-Japan Competitiveness and Resilience (CoRe) Partnership* (Apr. 16, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/16/fact-sheet-u-s-japan-competitiveness-and-resilience-core-partnership/.

(OpEx) savings[39]—Open RAN solutions also allow networks to be future-proofed and more easily upgradeable in the future.[40]

C. Open RAN Benefits

The Commission seeks comment on the benefits to be gained by access to interoperable networks.[41] Open RAN deployments have demonstrated comparable and, in many instances, superior performance to 4G and 5G systems employing a traditional RAN architecture, and there is no evidence to suggest that Open RAN system performance is likely to be negatively impacted due to multi-vendor environments. Open RAN deployments have demonstrated performance comparable to proprietary RAN systems, and may in some instances offer superior performance, especially for power consumption. [42] Open RAN deployment benefits wireless networks in many ways, including cost savings, network sharing, eliminating vendor lock-in and promoting competition, security, and third-party testing. Open RAN networks are scalable and can support from ten to millions of subscribers, depending on how many instances and substantiations of the Virtualized Network Functions ("VNFs") operators run on a single platform. Open RAN can run multiple operators using multiple VNFs, sitting side-by-side on the same platform to have

[39] iGR, Open RAN Integration: Run With It (2020) *in* Mavenir, Your Guide to OpenRAN 55-56 (2021) (citing Strategy Analytics study) (Mavenir e-book attached); Senza Fili Consulting, Future Proofing Mobile Network Economics—Assessing the TCO for Cloud RAN and Centralized RAN (2018) *in* Mavenir, Your Guide to Open RAN 114 (2021) (Mavenir e-book attached).

[40] As discussed below in the national security discussion, section II.G, this cost effectiveness is particularly important as the Commission works to implement the Secure and Trusted Communications Networks Act, a $1.9 billion initiative.

[41] *See* Open RAN NOI at 14, para. 32.

[42] When comparing equivalent configurations of D-RAN/C-RAN with Open RAN, Open RAN actually provides power savings through the use of inherent architecture changes described in the O-RAN Alliance fronthaul 7.2 specification that focus on reducing transmission bandwidth when there is lower traffic and power saving features, such as use of Section Type – for putting radio in low power mode when idle." Mavenir, Open RAN – Mature and Ready for Deployment (2021) *in* Mavenir, Your Guide to OpenRAN 67 (2021) (Mavenir e-book attached).

segregated networks. In the near future, network sharing via software will also benefit wireless operators.

In addition, Open RAN breaks open the interface between the remote radio head and the Distributed Unit,[43] eliminating vendor lock-in, *i.e.*, giving wireless operators freedom to choose. With the current legacy vendors, networks are a proprietary, walled garden. With open interfaces, Open RAN enables wireless operators to have full visibility and control of their network's end-to-end security. Open RAN interfaces, defined in the O-RAN technical specifications, provide increased independent visibility and the opportunity for a more secure system. Since the O-RAN Alliance builds on 3GPP's 5G architecture, it also benefits from 3GPP's advanced security features introduced for 5G.

Open RAN offers third party testing benefits as well. An O-RAN-specification radio will work with different suppliers' baseband, and each of the elements of the baseband can be tested independently because there is a defined specification; relieving wireless operators from needing to test in their own labs. Radios can then be purchased from any supplier and tested independently by third parties for functionality. This results in large cost savings for wireless operators which, in turn, creates competition, spurs innovation and lowers costs for consumers.

D. Costs and Deployability

With respect to the Commission's questions on operator resources,[44] Open RAN is more cost-efficient and less resource intensive compared with hardware-based proprietary networks. Consequently, Mavenir does not see the deployment and management of Open RAN as posing a challenge to wireless operators' resources. While wireless operators' networks vary, Open RAN

[43] "The Distributed Unit (DU) is where the real-time, baseband processing functions reside. The DU can be centralized or located near the cell site." Mavenir, Your Guide to OpenRAN 6 (2021) (Mavenir e-book attached).

[44] *See generally* Open RAN NOI at 20, para. 50 (seeking comment on network operator resources).

deployment, if anything, should result in the same draw on resources as the resources wireless operators draw upon to deploy proprietary networks.

Traditionally, wireless operators purchased hardware equipment and expensed it as a one-time capital expense that depreciated over time, but as networks have evolved, software and services have begun to replace hardware. As a result, wireless operators are expensing more on the operational side of the business. Fortunately, these ongoing operational costs are much lower than traditional hardware and proprietary software, which must be replaced when new services are required by the wireless operators. So, when the costs are netted out, Open RAN is not only less expensive to deploy due to CapEx savings, it is less expensive to operate because upgrades and new innovative service offerings can be deployed through software rather than changing out capital intensive—and expensive—hardware.

As noted above, with Open RAN and open interfaces, costs are lowered because equipment does not need to be replaced, nor networks scrapped over time. In addition, software defined radios and cores that are virtualized allow for software upgrades, easily allowing wireless operators to upgrade their networks to provide customers with new services and features. CapEx and OpEx are lowered in many cases. For example, wireless operators do not have to send crews to replace equipment on towers or at the base. Open RAN offers lower deployment times through automation, which can reduce the average time for deployment.[45] Open RAN also allows each wireless operator to have their own technology and feature roadmap, tailoring networks for individual operating needs. Accordingly, Open RAN reduces both CapEx and OpEx, and enables any size wireless operator—large or small—to operate,

[45] *See* iGR, Open RAN Integration: Run With It (2021) *in* Mavenir, Your Guide to OpenRAN 51 (2021) ("[A] virtualized RAN combined with centralization can be deployed faster than a traditional architecture since the only site installation required is for the radio and power. The remainder of the installation uses remote software loads managed through central operation center which do not require an additional site visit.") (Mavenir e-book attached).

upgrade, and expand their services to customers, to the effect of future-proofing U.S. wireless networks. Open RAN breaks the paradigm that one-size-fits-all.

E. Disaggregation and Integration

The Commission seeks comment on the impacts of disaggregation and component integration.[46] Disaggregation in software is common in the cloud, enterprise and core of the mobile network and is in large-scale use, and it enables more competition, lower costs, and more agile networks. RAN disaggregation allows for great flexibility and would not make Open RAN deployment any more complex than proprietary RAN deployment. The different components in an Open RAN architecture are similarly seamlessly integrated. Like proprietary RAN, Open RAN requires interoperability tests, and continuous improvement of integration efforts between hardware and software layers.

Open RAN deployment testing is no different than that of a proprietary RAN. Radios with 3GPP specifications on one side, and O-RAN specifications on the other will work with different vendors' baseband. As stated above, because there is a defined specification with 3GPP interfaces, those elements can be tested independently, which relieves wireless operators from testing in their own labs. Radios can thus be purchased from any supplier, tested independently

[46] *See* Open RAN NOI at 20, paras. 49, 50. iGR explains in the attached white paper that "disaggregation means separating the hardware from the software," as opposed to RAN systems built with "proprietary software and purpose-built hardware." iGR, Open RAN Integration: Run With It (2021) *in* Mavenir, Your Guide to OpenRAN 45 (2021) (Mavenir e-book attached). With respect to integration, "It is important to understand there are two levels of integration required when discussing Open RAN networks: Open RAN ecosystem integration includes the hardware, software, systems integrators[("SIs")], data centers and MNOs. In this case, the systems integrator will be responsible for integrating across the entire solution including integrating open radios. To ensure the ecosystem thrives and performs as required, the SI must be impartial and not aligned or associated with a specific hardware or software vendor. System integration of the Open RAN software on COTS [Commercial Off The Shelf] hardware. This level of integration is similar to what occurs in the data center environment. In fact, many of the same tools and principles are used, which further eases Open RAN adoption. In addition to this, multiple vendors from the ecosystem can come together to self-integrate and certify their solutions to create a blueprint that mobile operators can use directly into their networks." iGR, Open RAN Integration: Run With It (2021) *in* Mavenir, Your Guide to OpenRAN 52 (2021) (Mavenir e-book attached).

by a third party—with every assurance the radios will work—and on the basis that any wireless operator can buy them and not get locked into a specific supplier or system integrator.

After the integration is tested and complete, deployment complexity is no different than with proprietary RAN solutions. Open RAN system integration requires the same project management and network management skill—with the same associated costs as a proprietary RAN deployment, and can easily be accomplished by smaller wireless operators with less support. Wireless operators can either take responsibility for these integration efforts on their own, or work with Open RAN suppliers to handle this integration, or work with system integration companies.

F. Testbeds

Open RAN does not require testbeds, or any particular tests different from those imposed on proprietary RAN networks, equipment, or software.[47] None of the wireless generation technologies—2G, 3G, 4G, or 5G—underwent any public testbeds or proving before implementation. Because Open RAN can best be thought of as a better, open interface implementation of existing network architecture, there is really nothing to test—apart from the interface implementation—that is not already being tested, or has not been tested billions of times daily in real life by consumers. Aside from encouraging and implementing Open RAN deployment, the Commission should not have a different role in promoting, developing, or testing of Open RAN equipment. Open RAN does not require any different testing than current systems.

[47] *See generally* Open RAN NOI at 24-25, para. 63 (seeking comment on testbeds).

G. National Security and Supply Chain

Open RAN poses tremendous national security benefits that would allow the Commission and eligible providers to best implement the Commission's Reimbursement Program[48] to replace Huawei and ZTE equipment and services in U.S. networks. Moreover, "zero trust philosophy" (never trust, always verify), means Open RAN is inherently more secure and is a better solution than the opaque and exploitable proprietary RAN solution currently being employed.

H. Multiple Vendors' Effect on Supply Chain Security and Network Security

The Commission seeks comment on the extent to which Open RAN addresses "supply chain risk management issues and enable[s] the deployment of secure and reliable networks in the United States."[49] As Mavenir recently testified before Congress, "[t]he current U.S. RAN supply chain is a prized market – the highest margin and most profitable globally."[50] Open RAN opens networks to allow multiple vendors to provide equipment or services, and enables vendors to compete to provide those services and equipment. This multi-vendor approach prevents wireless operators and countries from becoming reliant on a single company to equip and service a network – referred to as "lock-in." This allows networks to be futureproofed: If a security issue arises—either with a component of the network or even perhaps with the viability of the supplier—it is far easier, and cost-effective, to remove the specific component as opposed to the

[48] *See generally, e.g.*, *Supply Chain Second Report and Order*, 35 FCC Rcd 14284.
[49] Open RAN NOI at 17, para. 40.
[50] *Leading the Wireless Future: Securing American Network Technology*: Hearing before the Subcomm. on Commc'ns & Tech. of the H. Comm. on Energy & Commerce, 117th Cong. (2021) (testimony of John Baker, Senior Vice President, Business Development, Mavenir), https://www.congress.gov/117/meeting/house/112475/witnesses/HHRG-117-IF16-Wstate-BakerJ-20210421-U1.pdf.

cost of ripping and replacing an entire network, as has been the case with Huawei and ZTE equipment and prevents a complete rip and replace happening again.

Management of multiple vendors is an efficient, easy process for wireless operators regardless of size.[51] As one example, SIs, such as Mavenir, manage end-to-end integration, simplifying the engagement for wireless operators and creating an offering that is on par with those of the traditional, hardware-centric proprietary vendors. Assertions of difficult vendor management in Open RAN architectures seem obviously to be nothing more than fearmongering by foreign-owned incumbents to discourage wireless operators from dealing with potential competitors.

In addition, Open RAN architectures enable wireless operators to remove or change components in a faster and more cost-effective manner as opposed to the removal of proprietary hardware-based equipment. To replace hardware, crews of workers must be dispatched to remove equipment from towers; software-based networks mitigate these costs, reducing the need for costly truck rolls, and allowing the software to simply be replaced and upgraded at remote locations.

An Open RAN software vendor supply chain excluding untrusted entities also removes concerns regarding "software running over hardware of an untrusted vendor,"[52] as that supply chain is more readily observable and can be independently tested. Indeed, Open RAN architectures are actually more secure than proprietary systems. In proprietary systems, only the

[51] *See, e.g.*, Triangle Communications Comments, WC Docket No. 18-89, at 3 (Apr. 9, 2021) ("Installation of SSPV [sole-source proprietary vendor] equipment necessitates interaction with various, seemingly non-interconnected, departments within the SSPV. When a network problem arises, the situation invariably devolves into intra-company, inter-divisional finger pointing as the cause of the problem is investigated. At the end of the day, Triangle chases down the various finger points to locate the cause of the problem. Triangle understands this to be the nature of the beast, the equipment and connections are immensely complex, and Triangle does not mean to imply any level of dissatisfaction with this process or with any SSPV. Triangle's point is that Triangle does not see how working with multiple ORAN vendors would differ materially in this regard.").

[52] Open RAN NOI at 17, para. 40.

company that makes the product can test its network security or have visibility into its operations. That means no one other than the supplier would know for sure if there are security issues unless the supplier discloses it. Open interfaces, on the other hand, are auditable and verifiable by third parties and wireless operators. This gives wireless operators and other third-party suppliers confidence that security tests have met specific requirements and allows for ongoing monitoring.

In addition, because most Open RAN solutions are virtualized, they feature several new cloud-based security controls that make networks more resilient, like sandboxing, and containerization.[53] Mavenir uses multiple sources to verify the security of its Open RAN products. The open nature of this approach means network operators are able to audit and verify the technology independently as they deploy it in their networks.

There is also no evidence that Open RAN deployments would "expose new security vulnerabilities that might not otherwise exist in a more closed architecture"[54] As noted in the consortium white paper, *Security in OpenRAN*, Open RAN is rooted in the concept of zero-trust, employing the principle of "never trust, always verify."[55] "Zero Trust is designed to protect modern digital environments by leveraging network segmentation, preventing lateral movement, providing Layer 7 threat prevention, and simplifying granular user-access control."[56]

[53] "Sandboxing is a software management strategy that isolates applications from critical system resources and other programs." TechTerms, Sandboxing, https://techterms.com/definition/sandboxing (last visited Apr. 16, 2021). "Containerization is a type of virtualization strategy that emerged as an alternative to traditional hypervisor-based virtualization. As with the latter, container-based virtualization involves creating specific virtual pieces of a hardware infrastructure, but unlike the traditional approach, which fully splits these virtual machines from the rest of the architecture, containerization just creates separate containers at the operating system level." Techopedia, Containerization, https://www.techopedia.com/definition/31234/containerization-computers (last visited Apr. 28, 2021).

[54] Open RAN NOI at 20, para. 51.

[55] Mavenir, Security in OpenRAN (2021) *in* Mavenir, Your Guide to OpenRAN 85 (2021) (Mavenir e-book attached).

[56] *Id.* NIST's abstract to Special Publication 800-207, Zero Trust Architecture, explains that "Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to

The recent SolarWinds cyberattack is a prime example of why open architectures provide more security benefits than proprietary architectures. In SolarWinds, Orion provided a proprietary software-based monitoring product. Proprietary software has been described as "a black box where you can never know what's really going on" and "is now, always has been, and always will be more of a security problem."[57] Open architectures allow more eyeballs to watch the network and are auditable and verifiable by third parties and network operators. The introduction of more stakeholders does not introduce vulnerabilities—open architectures promote collaboration and multi-vendor monitoring of networks; the software is fully vetted by vendors. This visibility is the inherent security benefit of Open RAN.

I. USF and the Secure Networks Reimbursement Program

The Commission seeks comment on possible additional steps to support Open RAN deployment as a solution to replace non-secure equipment and services in the Supply Chain Second Report and Order.[58] Mavenir appreciates the Commission's support in making Open RAN an eligible reimbursement at its December 2020 meeting. At that meeting, Commissioner Starks proposed requiring providers to certify that they have considered Open RAN for their

focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established. Zero trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that are not located within an enterprise-owned network boundary. Zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource." NIST Information Technology Laboratory, Computer Security Resource Center, *SP 800-207, Zero Trust Architecture*, https://csrc.nist.gov/publications/detail/sp/800-207/final (last visited Apr. 15, 2021). *See also* NIST Special Publication 800-207, Zero Trust Architecture, https://doi.org/10.6028/NIST.SP.800-207.

[57] Steven J. Vaughan-Nichols, SolarWinds, the World's Biggest Security Failure and Open Source's Better Answer, The New Stack (Dec. 18, 2020 2:01pm), https://thenewstack.io/solarwinds-the-worlds-biggest-security-failure-and-open-sources-better-answer/

[58] *See* Open RAN NOI at 25, para. 65.

networks.[59] Mavenir strongly supports this proposal and recognizes that Open RAN's lower costs can help stretch limited federal funds even further, a benefit that was recognized by a bipartisan group of nine senators.[60] The Commission should further act to prioritize Open RAN adoption and to encourage its adoption. As U.S. Representatives Doris Matsui, Brett Guthrie, Anna Eshoo, and Cathy McMorris Rodgers wrote the Commission in September 2020, "this moment presents a critical opportunity to secure and widen our mobile network supply chain by providing as many options as possible for impacted carriers."[61]

Mavenir agrees in principle with the Commission's assertion that it believes "including Open RAN and other virtualized equipment and services could help promote Open RAN development and deployment."[62] However, Mavenir is concerned with many unintended consequences at odds with policymakers' original intent for the Secure Networks Reimbursement Program. Policymakers sought to facilitate supplier diversity, advance U.S. leadership in 5G, and encourage the adoption of new technologies. However, impacted wireless operators appear to be opting for foreign equipment based on a proprietary system, continuing to lock out U.S. suppliers due to policy time constraints and no use of a budget definition, further solidifying the current duopoly's control over the RAN market.

This is a critical opportunity to facilitate supplier diversity and future-proof U.S. networks so that the U.S. does not run the risk of another "rip and replace" in the future. Congress and the Commission required the replacement of untrusted suppliers because wireless

[59] *Supply Chain Second Report and Order*, 35 FCC Rcd at 11424 (Statement of Commissioner Starks).
[60] *See* Letter from Mark R. Warner et al., U.S. Senator, to Ajit Pai, Chairman, FCC (Oct. 1, 2020), https://www.warner.senate.gov/public/_cache/files/e/2/e2f06906-cf9a-4fc1-ae3d-ae48624e69e1/F9A2276A40CFAC8D7365C68A8258C728.openran-letter-to-the-fcc-10-1.-docx.pdf
[61] Letter from Doris Matsui et al., U.S. Representative, to Ajit Pai, Chairman, FCC (Sept. 24, 2020), https://matsui.house.gov/uploadedfiles/20200924_-_open_ran_rr_letter.pdf.
[62] Open RAN NOI at 26, para. 66.

operators became too reliant on a small number of suppliers due to market factors and consolidation.[63] By allowing consolidation and by not taking steps to promote competition in the communications supply chain, especially among U.S. suppliers, the U.S. effectively eliminated the opportunity to participate in the global RAN market and fall behind globally in mobile infrastructure specification and development. Through the Supply Chain Reimbursement Program and the US Telecom Act, Congress created laws to promote the use of funding to provide U.S. wireless operators with an opportunity to use U.S. suppliers to build U.S. networks to replace untrusted foreign-owned suppliers. The Commission should incentivize these wireless operators to utilize this funding to do so. By requiring all suppliers to adhere to open and interoperable interfaces, which help to secure and futureproof our networks, the Commission will allow wireless operators to quickly pivot should issues arise, for example, arising from vendor instability or national security concerns.

To encourage Open RAN deployment and development through the Reimbursement Program, the Commission should prioritize a policy of replacement equipment with published open and interoperable interfaces under FRAND (fair, reasonable, and non-discriminatory) licensing terms, giving preference to U.S. suppliers in order to get back to a level playing field. Contrary to some claims,[64] this is not a technology mandate. Open and interoperable interfaces

[63] *See generally*, John Shinal, *Alcatel to buy Lucent for $13.5 billion*, MarketWatch (Apr. 3, 2006, 12:21 PM) https://www.marketwatch.com/story/alcatel-to-acquire-lucent-for-135-billion-in-stock (Alcatel acquisition of Lucent); Ian Austen, *Nortel Seeks Bankruptcy Protection*, NYTimes (Jan. 14, 2009) https://www.nytimes.com/2009/01/15/technology/companies/15nortel.html (Nortel bankruptcy); *Nokia, Siemens to merge units*, Cnet (June 25, 2006 9:00 AM), https://www.cnet.com/news/nokia-siemens-to-merge-units/ (Nokia-Siemens merger); Terhi Kinnunen & Leila Abboud, *Nokia to buy out Siemens equipment venture; shares surge*, Reuters (July 1, 2013, 12:20 AM), https://www.reuters.com/article/us-nokia-siemens/nokia-to-buy-out-siemens-equipment-venture-shares-surge-idUSBRE96004F20130701 (eventual buyout of Siemens 50% stake); *Nokia's $16.6 Billion Acquisition Of Alcatel-Lucent Explained*, Forbes (Apr. 16, 2015, 01:36 PM), https://www.forbes.com/sites/greatspeculations/2015/04/16/nokias-16-6-billion-acquisition-of-alcatel-lucent-explained/?sh=795a7068605c (Nokia acquisition of Alcatel-Lucent).

[64] *See, e.g.*, Rene Summer, Mobile Radio Access Networks: What Policy Makers Need to Know, Ericsson Blog (Sept. 17, 2020), https://www.ericsson.com/en/blog/2020/9/ran-what-policy-makers-need-to-know ("policy makers

are not a technology; they are a policy/principle for the architecture upon which networks can be built and the supply chain can be expanded. Open interface and interoperable principles are already in use by wireless operators globally for their mobile cores. If the Commission took additional steps to encourage Open RAN deployment and development through the Reimbursement Program, Open RAN's lower cost would mean limited federal funds would be stretched even further due to lower replacement costs. Additional Commission steps would open the U.S. RAN market to U.S. and other suppliers and grow the Open RAN ecosystem based on the principles of competition. The UK's Telecom's Diversification Taskforce, tasked by that nation's Secretary of State to "to chair an expert Taskforce for around six months to identify solutions and opportunities to diversify the supply market for 5G,"[65] has just issued recommendations on supply chain diversification. Among other recommendations, that taskforce recommends that the UK government:

- "[S]et the conditions" to attract at least one "and ideally two" new scale vendors;
- Set an "aspiration" for a 25% OpenRAN market share deployment in the UK;
- "[S]eek commitments with regards to their [UK mobile network operator] 5G supplier diversity and open architecture adoption . . . [and] The Government's objective must be to have the operators adopt and publish their supplier diversity and open architecture roadmaps";
- Introduce "'provenance' standards on vendors so that network operators can understand and maintain records of the source country and vendors of the products they deploy into UK 5G networks." [66]

Likewise, the Open RAN NOI is a perfect opportunity for the Commission to spur the U.S.—and the world—to adopt greater supply chain diversity and innovation. Because the U.S. is

should not pick winners, but continue to ensure the following outcomes: . . . Technology-neutral regulation, not mandating any architecture.").

[65] Telecoms Diversification Taskforce, Findings and Report 2 (2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975007/April_2021_Telecoms_Diversification_Taskforce_Findings_and_Report_v2.pdf.

[66] *Id*. at 12-13, 15.

traditionally a global technology leader, any Commission actions in the area will instill global confidence, and permit U.S. suppliers to enter the global market as the world follows the Commission's lead.

To encourage providers to deploy Open RAN technology,[67] the Commission could adopt Commissioner Starks' proposal to require wireless operators to certify that they have considered Open RAN for their networks. The Commission could also require prioritization of funds to those wireless operators that utilize Open RAN; require cost considerations in decision-making; incentivize Open RAN deployment; incentivize wireless operators with the use of U.S. funds for Open RAN only; or require wireless operators to prefer U.S. suppliers to level the playing field in the U.S.

As the Commission notes in the Notice of Inquiry, the Secure Networks Act imposes short deadlines, but allows for individual providers deadline extensions in "limited circumstances."[68] Because of the fear, uncertainty, and doubt ("FUD") and confusion created in the marketplace by the current duopoly, wireless operators do not have complete confidence in meeting the Commission's current timeline. Granting wireless operators that choose to deploy Open RAN an extension of time of 12 months could incentivize smaller operators to deploy Open RAN. Regardless of the extension, further action by the Commission is needed to incentivize, prioritize, or require Open RAN adoption.

Mavenir disagrees with the Commission's assertion that it expects "that providers may incur increased upfront costs for this [Open RAN] equipment,"[69] as there are no increased upfront costs incurred. As far as other costs the Reimbursement Program could cover, it could

[67] *See* Open RAN NOI at 27, para. 68.
[68] *Id*.
[69] *Id*. at para. 69.

cover development NRE (non-recurring engineering costs); component-specific development costs to compensate for lack of domestic product, as well as expenses for system integrators to configure carrier network infrastructure. Wireless operators deploying Open RAN will not encounter extraordinary expenses; their expenses will be the same or less than those incurred for proprietary networks.

III. Market Issues and Cost-Benefit Analysis

The current equipment market is one posing barriers to entry for new entrants, and one where existing operators are compelled by incumbent suppliers to only use incumbent equipment and services. The cost benefit analysis favors Commission action to remove these barriers to entry.

A. Market Issues

Mavenir now addresses the Commission's questions on Open RAN's effect on market entry, vendor diversity, and the state of competition.[70] By its nature, Open RAN facilitates multi-vendor diversity and grows competition. The Open RAN Policy Coalition (ORPC)'s diverse membership, which numbers more than 60 companies, demonstrates the demand for open and interoperable interfaces. There is restricted competition in the U.S.'s wireless networks today. With the ban on Huawei and ZTE, there are essentially two companies – both foreign-headquartered – who manufacture and service RAN equipment for the entire United States RAN market. Because of the proprietary nature of their equipment, other suppliers, including U.S.-headquartered companies, are locked out of the RAN. This RAN equipment is not interoperable with other vendor's hardware and software. There are limited instances where one of the two foreign-owned incumbents have extended their proprietary

[70] *See* Open RAN NOI at 14, para. 31.

system to one or two other companies, but even that system remains proprietary and is not a true Open RAN system.[71]

Proprietary equipment restricts wireless operator choices and options, allowing one or two foreign-owned incumbents to control operator relationships and achievements. Open RAN will resolve the current lack of competition and help a wider ecosystem to flourish. Open interfaces will drive technical innovation, resulting in commercial competition. The replacement of 3G and 4G LTE Huawei and ZTE equipment and services, along with U.S. 5G deployments are opportunities to make a difference and inject competition into the supply chain. If the Commission does not require or incentivize Open RAN deployment now, this narrow window for market access will close, locking U.S. suppliers out of the RAN market for a generation or more. This is a critical juncture where we can grow a U.S.-based ecosystem and futureproof our networks to prevent another rip and replace in the future.

Lower wireless operator costs are a natural outcome of competition. Competition in the wireless network equipment marketplace would also remove the risks inherent in the current dependency on foreign vendors. The Commission seeks comment on the 5G RAN market shares.[72] The Notice of Inquiry cites that "[b]y some estimates, Open RAN currently captures 9.4% of the total 4G and 5G market."[73] This market share is expected to increase once competition is introduced and barriers eliminated.

Given proprietary RAN's relatively higher cost compared to Open RAN, market share measures based on revenue are also skewed, and likely understate Open RAN's actual market

[71] *See Ecosystem Building: Samsung and Nokia Work Together to Conduct 5G Interoperability Testing*, Samsung (Feb. 24, 2017), https://www.samsung.com/global/business/networks/insights/blog/ecosystem-building-samsung-and-nokia-work-together-to-conduct-5g-interoperability-testing/.

[72] *See* Open RAN NOI at 15, para. 34.

[73] *Id.*

share. A better measure of growth is comparing the number of Open RAN *deployments*. Globally, 23 wireless operators have adopted or are trialing Open RAN, potentially covering some 1.3 billion subscribers, or 25.2% of the world's subscriber base.[74] While these metrics are highly encouraging, they unfortunately do not include the U.S. market, which the Commission and other federal stake holders must address.

B. Cost Benefit Analysis

In considering its Open RAN cost benefit analysis,[75] Mavenir asks that the Office of Economics and Analytics ("OEA") take into account the costs of using and replacing insecure foreign equipment, in addition to the CapEx and OpEx costs savings Mavenir outlined above.[76] For example, if wireless operators had used open interface equipment instead of non-secure equipment—and preferred domestic suppliers due to lower costs—the U.S. would have saved the $1.9 billion that is now going to fund the Supply Chain Reimbursement Program. Additionally, OEA should account for the costs wireless operators would not have otherwise incurred in not having to inventory, replace equipment, and incur other rip and replace compliance costs; or costs to mitigate network breaches by foreign state- or state-sponsored actors due to unsecure equipment.

Wireless operators will benefit from open interfaces and standards. This will allow wireless operators to more readily source secure equipment, made more cost effective due to competition, and future proofed due to competitive innovation.

[74] iGR, Open RAN Integration: Run With It 1 (2021).

[75] *See generally* Open RAN NOI at 33, para. 87 (inquiring on OEA plans for an economic study on Open RAN development).

[76] *See* section II.B above.

The Commission seeks comment "on the relative and absolute costs of Open RAN deployment and interoperability."[77] Open RAN equipment CapEx costs are less with the added benefit of lower operating expenses once deployed, resulting in the cost efficiencies of nearly 40% in CapEx and 34% in OpEx savings.[78] Wireless operators are ultimately bringing a lower cost of service to their subscribers. High margin equipment (margin stacking) leads to higher consumer pricing. By way of illustration, an incumbent vendor gets radio and other components from smaller vendors, compiles it with margin on top. With Open RAN however, a wireless operator can work directly with multiple vendors to eliminate margin stacking, resulting in better profitability. The United States has one of the most expensive network RAN equipment in the world; presenting a very lucrative market for incumbent vendors.

As for costs due to using multiple vendors,[79] network design and integration is a cost irrespective of whether it is a proprietary or open network; there is no change in the costs incurred, no matter what architecture is used.

Regarding how "interoperability between the various equipment vendors can be ensured,"[80] interoperability can be ensured through vendor cooperation, through OTIC (ORAN Technical Integration Centers), through TIP labs, and other testing and interoperability mechanisms still to be defined.

[77] Open RAN NOI at 32, para. 88.

[78] iGR, Open RAN Integration: Run With It (2020) *in* Mavenir, Your Guide to OpenRAN 55-56 (2021) (citing Strategy Analytics study) (Mavenir e-book attached); Senza Fili Consulting, Future Proofing Mobile Network Economics—Assessing the TCO for Cloud RAN and Centralized RAN (2018) *in* Mavenir, Your Guide to Open RAN 114 (2021) (Mavenir e-book attached).

[79] *See* Open RAN NOI at 33-34, para. 88.

[80] *Id*. at 34, para. 88.

IV. Legal Issues

The market barriers, national security and supply chain issues, and the state of the RAN ecosystem present ripe and urgent opportunities for Commission action. The Commission has legal authority under Title III and CALEA; sections 201(b) and 254 of the Communications Act; and section 706 of the 1996 Act, to ensure U.S. networks remain secure and competitive.

A. Title III and CALEA

The Commission has authority under Title III and CALEA to mandate Open RAN adoption, or at the very least, give operators the choice to opt for Open RAN. As the Commission states in the Notice of Inquiry, the Commission has "broad authority under Title III to manage radio spectrum and prescribe nature of wireless services to be rendered, and modify existing licenses when doing so would promote the public interest."[81] Under Title III, the "public convenience, interest, [and] . . . necessity requires"[82] the Commission to mitigate the issues presented by allowing two foreign equipment vendors to dominate the market, which as noted poses significant competitive and national security concerns. The Commission routinely uses its authority under Title III to address competitive issues and market concentration in communications-related markets. Here, the Commission should use its Communications Act authority to address the now highly concentrated RAN duopoly, which of course, is the critical component of every wireless network in the country. The most straightforward way of doing so is adopt policies, as urged herein, that foster the adoption of multi-vendor Open RAN networks in the U.S. and eliminate barriers to their deployment. The public interest, convenience, and necessity thus requires the Commission to take action by using its broad Title III authority to

[81] Open RAN NOI at 32, para. 84 (citing 47 U.S.C. §§ 301, 302, 303, 309).
[82] 47 U.S.C. § 303.

ensure a level playing field for the mobile infrastructure market which includes the RAN and the mobile core.[83]

Further, the Communications Assistance Law Enforcement Act (CALEA), is an avenue the Commission can also pursue to facilitate, and eliminate barriers to Open RAN deployment. The Notice of Inquiry notes that CALEA section 105 was implicated when the Commission adopted its prohibition on using Universal Service Fund (USF) funds to "purchase, maintain, or operate covered communications equipment and services,"[84] and carriers thereby have a duty to "avoid the risk that an untrusted supplier could illegally intercept or provide remote unauthorized network access by the insertion of malicious hardware or software implants."[85] The current proprietary RAN network is opaque. No one but the incumbent equipment manufacturer has visibility over the individual pieces of equipment or software code in the RAN, nor are operators free to remove that equipment or software. In contrast, an Open RAN operator can "deploy the latest security tools for monitoring vulnerabilities and automated remediation measures as required,"[86] and replace equipment and software as needed. Open RAN provides complete

[83] *Id*. The Commission also has broad authority under sections 151, 251, and 256 of the Communications Act to prohibit discrimination among carriers for purposes of interconnecting with other carriers to ensure transparency across networks. Specifically, Section 151 states that the Commission was created, *inter alia*, "for the purpose of the national defense, for the purpose of promoting safety of life and property through the use of wire and radio communications." 47 U.S.C. § 151. Section 251 establishes that common carriers have the duty "(1) to interconnect directly or indirectly with the facilities and equipment of other telecommunications carriers; and (2) *not to install network features, functions, or capabilities that do not comply with the guidelines and standards established pursuant to section 255 or 256 of this title*." 47 U.S.C. § 251(a) (emphasis added). Section 256 provides that its purpose is to "(1) *to promote nondiscriminatory accessibility by the broadest number of users and vendors of communications products and services to public telecommunications networks used to provide telecommunications service* through--(A) coordinated public telecommunications network planning and design by telecommunications carriers and other providers of telecommunications service; and (B) public telecommunications network interconnectivity, and interconnectivity of devices with such networks used to provide telecommunications service; and (2) to ensure the ability of users and information providers to seamlessly and transparently transmit and receive information between and across telecommunications networks." 47 U.S.C. § 256(a) (emphasis added).

[84] Open RAN NOI at 32, para. 84.

[85] *Id*.

[86] Mavenir, Security in OpenRAN (2021) *in* Mavenir, Your Guide to OpenRAN 101 (2021) (Mavenir e-book attached).

visibility and control over the network, allowing wireless operators to comply with section 105 of CALEA. As such, the Commission should act to allow carriers to secure their networks against malicious hardware and software, or the unknown exploitation of their present RAN networks.

B. Sections 201(b) and 254

Sections 201(b) and 254 of the Communications Act provides the Commission the authority to encourage and incentivize development and deployment of Open RAN and virtualized networks as it relates to securitizing U.S. networks similar to the authority used in the *Supply Chain Proceeding*.[87] The *Supply Chain Second Report and Order* cites the following as legal authority under these two sections:

> 47 U.S.C.§ 201(b) ("All charges, practices, classifications, and regulations for and in connection with such communication service, shall be just and reasonable . . . . The Commission may prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of this chapter.");
>
> § 254(b) ("The Joint Board and the Commission shall base policies for the preservation and advancement of universal service on the following principles: (1) Quality services should be available at just, reasonable, and affordable rates; (2) Access to advanced telecommunications and information services should be provided in all regions of the Nation; . . . (7) Such other principles as the Joint Board and the Commission determine are necessary and appropriate for the protection of the public interest, convenience, and necessity and are consistent with this chapter.").[88]

The present proprietary RAN system does not allow for just and reasonable practices under section 201. Moreover, under section 254(b), if, as Mavenir outlines above in its cost discussion, Open RAN presents any additional cost benefits, and equipment manufacturers purposely shackle wireless operators to higher-cost equipment, how can it be reasonable and affordable to

[87] *See* Open RAN NOI at 33, para. 86. *See also Supply Chain Proceeding*.

[88] *Supply Chain Second Report and Order*, 35 FCC Rcd at 14291 n.41 (2020). *See also* 47 U.S.C. § 254.

pass these rates to consumers when lower-cost solutions are available now? Under section 254(b)(2), Open RAN will lower operating expenses and capital expenses, allowing and encouraging existing operators and new entrants to expand services to unserved and underserved areas, thus ensuring "Access to advanced telecommunications and information services should be provided in all regions of the Nation." Furthermore, as covered in the Title III discussion above, ensuring and maintaining access to secure, proven, and readily available wireless networks via Open RAN is truly in the public interest; burdening the public with non-competitive, non-U.S. vetted technology is not.

C. Section 706

Finally, as the Commission points out, section 706 of the 1996 Telecommunications Act directs the Commission to "encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans . . . by utilizing, in a manner consistent with the public interest, convenience, and necessity, price cap regulation, regulatory forbearance, measures that promote competition in the local telecommunications market, or other regulating methods that remove barriers to infrastructure investment."[89] The state of the RAN ecosystem is such that two foreign-owned incumbent equipment manufacturers have created a duopoly over time by adopting practices that limit their customers to only using their proprietary RAN. This is an absolute barrier to wireless infrastructure investment. The Commission should leverage its section 706 authority to permit all ecosystem participants—vendors, software developers, wireless operators and others—to invest in open interfaces that will increase competition in the wireless market and lower costs.

[89] Open RAN NOI at 33, para. 86 (quoting 47 U.S.C. § 1302(a)).

V. **CONCLUSION**

In sum, the Commission should immediately proceed to a Notice of Proposed Rulemaking in this proceeding. The RAN market has coalesced around two foreign-owned incumbents, who use their market power to dictate the equipment and services wireless operators can use in deploying and employing their networks—and have enjoyed high profits in the process. The Commission has ample legal authority to facilitate competitive entry through Open RAN deployments that will eliminate this duopoly, and foster security, innovation, and competition by incentivizing operators to deploy Open RAN in their wireless networks.

By: */s/ Caressa D. Bennet*
Caressa D. Bennet
E. Alex Espinoza
Womble Bond Dickinson (US) LLP
1200 19th Street, N.W.
Suite 500
Washington, D.C. 20036
(202) 467-6900

Counsel for Mavenir Systems, Inc.

Dated: April 28, 2021

MAVENIR™

YOUR GUIDE TO OPENRAN

April 2021
v1.0

Table of Contents

WHITE PAPERS AND SOLUTION BRIEFS

Introduction

We are pleased to share a compilation of documents that should help you as you consider the opportunity to deploy OpenRAN. This document has been compiled from white papers that summarize various aspects, including technical deployment, power consumption, security, total cost of ownership (TCO) analysis and system integration. These papers have been produced in conjunction with the world's leading experts, competitors, and partners to preset a well balanced compilation.

Should you have any detailed questions please do not hesitate to reach out us.

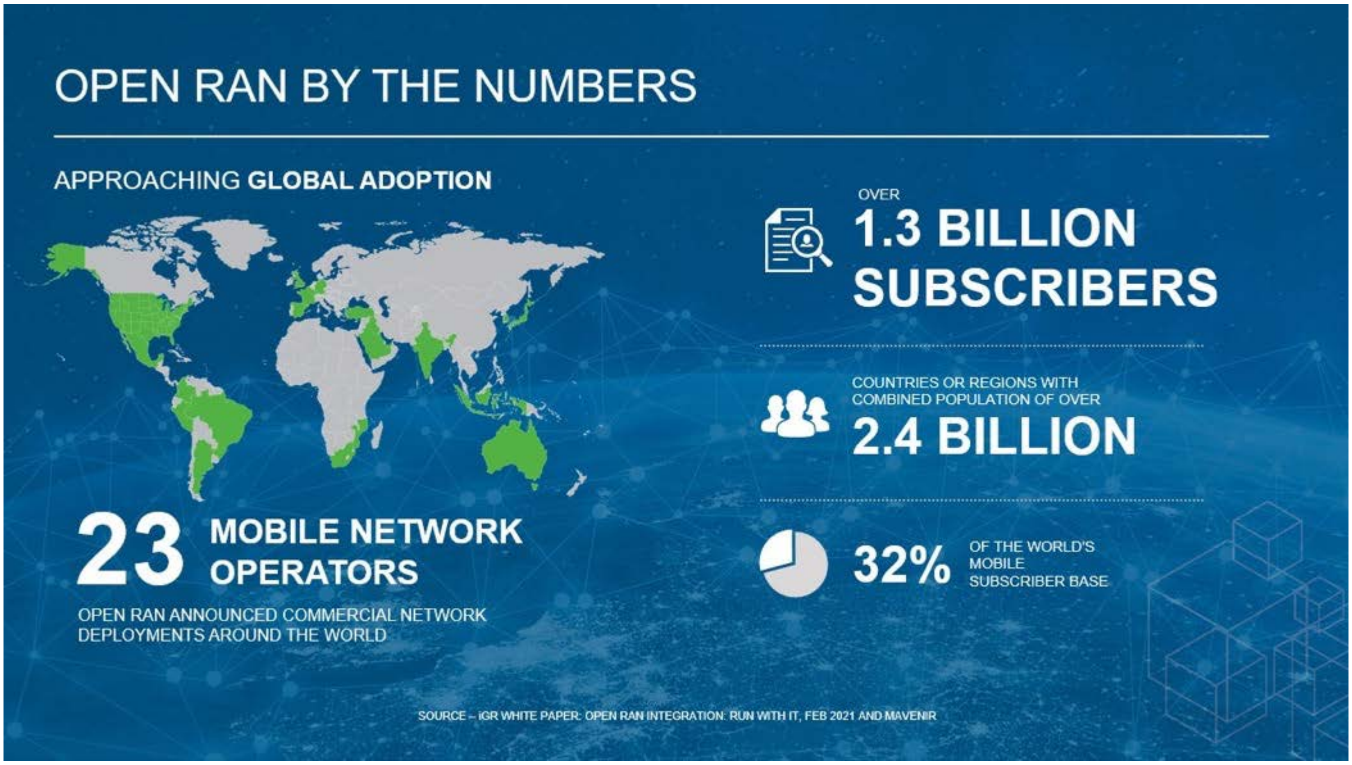
John Baker
Senior Vice President of Business Development
www.mavenir.com

Accelerating Network Transformation with Cloud-Native OpenRAN

OpenRAN principles present an alternative way of building networks that ensures interoperability, vendor competition, element security and reduced operating costs across the radio access networks (RAN).

OpenRAN focuses on using vendor-neutral hardware and software based on open interfaces and community-developed standards, giving operators the ability to use one supplier's radios with another supplier's RAN applications. With 5G deployment plans in full-swing, operators around the globe are using the opportunity to transform their mobile network (see Figure 1). Mavenir's vRAN OpenRAN solution is the world's first fully containerized, virtualized OpenRAN Split 7.2 architecture. It leverages open interfaces, virtualization, and web-scale containerization to support various deployment scenarios – including public cloud, private cloud, resulting in nearly 40% savings in TCO over five years.

Figure 1.



OPEN RAN BY THE NUMBERS

APPROACHING **GLOBAL ADOPTION**

23 **MOBILE NETWORK OPERATORS**

OPEN RAN ANNOUNCED COMMERCIAL NETWORK DEPLOYMENTS AROUND THE WORLD

OVER **1.3 BILLION SUBSCRIBERS**

COUNTRIES OR REGIONS WITH COMBINED POPULATION OF OVER **2.4 BILLION**

32% OF THE WORLD'S MOBILE SUBSCRIBER BASE

SOURCE – iGR WHITE PAPER: OPEN RAN INTEGRATION: RUN WITH IT, FEB 2021 AND MAVENIR

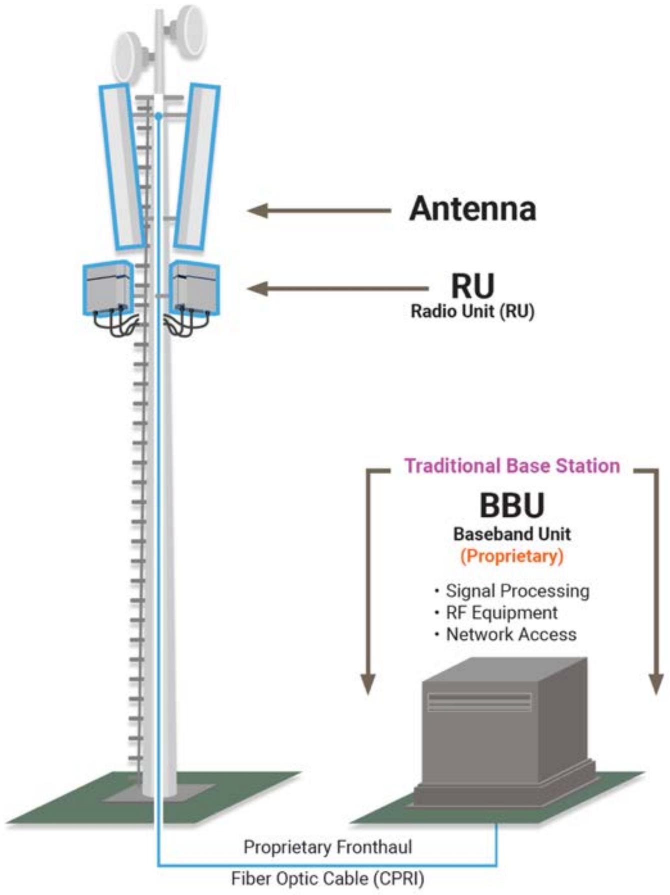
What is OpenRAN?

Open radio access networks, or OpenRAN, refers to a disaggregated approach to deploying mobile networks by using open and interoperable protocols and interfaces that allows for increased flexibility over traditional RAN systems. OpenRAN can be implemented with vendor-neutral hardware and software-defined technology based on open interfaces and industry-developed standards.

Traditional RAN

In a traditional RAN system, the radio, hardware, and software are proprietary (see Figure 2**)**. This means that nearly all of the equipment comes from one supplier and that operators are unable to, for example, deploy a network using radios from one vendor with hardware and software from another vendor.

Figure 2.



Mixing and matching cell sites from different providers typically leads to a performance reduction. The result is that most network operators, while supporting multiple RAN vendors, will deploy networks using a single vendor in a geographic region.

Proprietary

Closed & Embedded Interfaces

Pre-Defined Functionality

Single Vendor

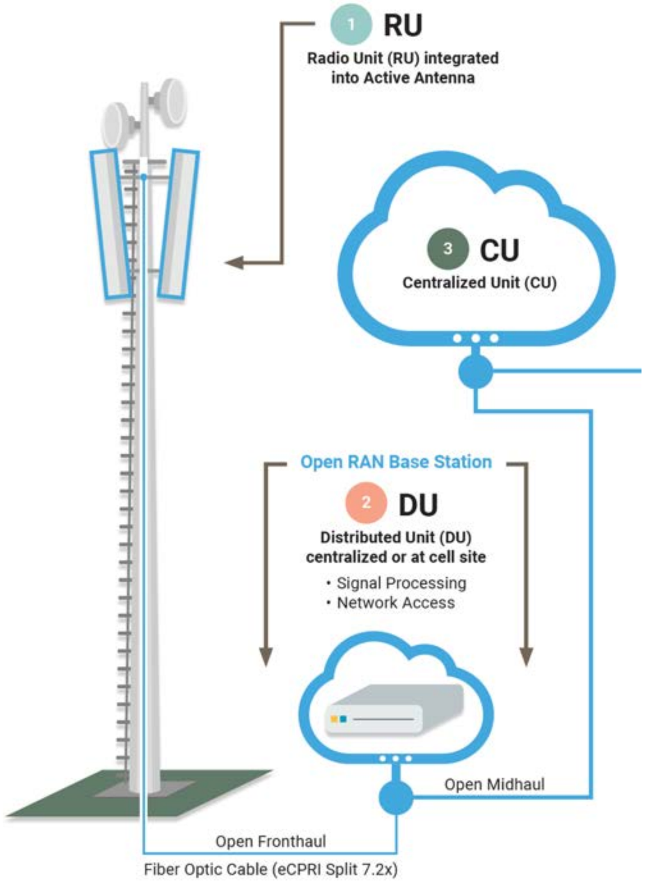
OpenRAN

OpenRAN is not a technology, but rather an ongoing shift in mobile network architecture that allows networks to be built using subcomponents from a variety of vendors. The key concept of OpenRAN is “opening” the protocols and interfaces between the various subcomponents (radios, hardware and software) in the RAN. As a technical matter this is what the industry refers to as a disaggregated RAN. The benefits of this approach include increased network agility and flexibility, increased innovation and cost savings (see Figure 3).

There are three primary elements in the RAN:

1. **The Radio Unit (RU)** is where the radio frequency signals are transmitted, received, amplified and digitized. The RU is located near, or integrated into, the antenna.
2. **The Distributed Unit (DU)** is where the real-time, baseband processing functions reside. The DU can be centralized or located near the cell site.
3. **The Centralized Unit (CU)** is where the less time-sensitive packet processing functions typically reside.

Figure 3.


1 RU
Radio Unit (RU) integrated into Active Antenna
3 CU
Centralized Unit (CU)
Open RAN Base Station
2 DU
Distributed Unit (DU) centralized or at cell site
• Signal Processing
• Network Access
Open Midhaul
Open Fronthaul
Fiber Optic Cable (eCPRI Split 7.2x)

It is the interfaces between the RU, DU and the CU that are the main focus of OpenRAN. By opening and standardizing these interfaces (among others in the network), and incentivizing implementation of the same, you can move to an environment where networks can be deployed with a more modular design without being dependent upon a single vendor. Making these changes can also allow the DU and CU to be run as virtualized software functions on vendor-neutral hardware.

Software Defined
Unbundled & Open Interfaces
Programmable & Flexible
Multi-Vendor Friendly

The Benefits of OpenRAN vRAN

COST SAVINGS. You can build a virtualized network, containerize it and each of the elements can be completely broken down. This modern network can support anywhere from tens of subscribers to millions of subscribers. It just depends on how many instances and substantiations of the virtual network functions (VNFs) and cloud-native network functions (CNFs) can you run on a single platform.

MULTIPLE OPERATORS & NETWORK SHARING. OpenRAN vRAN can run multiple operators using multiple VNFs/CNFs sitting side-by-side on the same platform to create segregated networks. Another benefit is network sharing in the future through software.

ELIMINATE VENDOR LOCK-IN. OpenRAN breaks open the interface between the remote radio head and the DU. With current legacy vendors, it's a walled garden and proprietary. Through O-RAN, a fully open interface on Split 7.2 has been defined including all the OEM.

SECURITY. OpenRAN provides operators with full visibility and control of their network's end-to-end security. OpenRAN interfaces, defined in the O-RAN technical specifications, provide increased independent visibility and the opportunity for an overall enhanced and more secure system. Since the O-RAN Alliance builds on 3GPP's 5G (New Radio) NR architecture, it benefits from 3GPP's advanced security features introduced for 5G.

3rd PARTY TESTING BENEFITS. Radios with 3GPP specs on one side and O-RAN specs on the other will work with different vendors' baseband and because there is a defined specification with 3GPP interfaces, the elements can be tested independently. This takes pressure off operators to test in their own labs. Radios can be purchased from any vendor and tested by independently by a 3rd party and can be assured that it works. Soon radios will be produced at low cost on the basis that any operator can buy them and not get locked into a specific system integrator.

What is the Difference Between OpenRAN, O-RAN and vRAN?

OpenRAN

Disaggregated RAN functionality built using open interface specifications between elements. Can be implemented in vendor-neutral hardware and software-defined technology based on open interfaces and community-developed standards.

O-RAN

Refers to the O-RAN Alliance or designated specification. O-RAN Alliance is a specification group defining next generation RAN infrastructures, empowered by principles of intelligence and openness.

vRAN

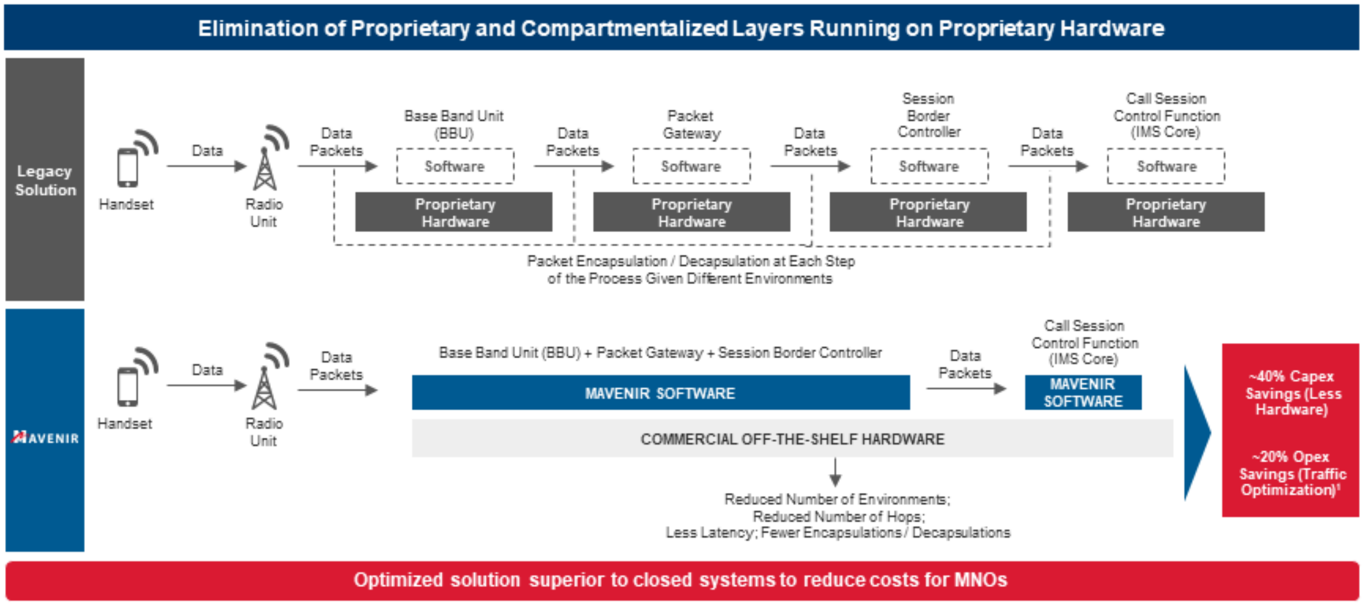
An implementation of the RAN in a more open and flexible architecture which virtualizes network functions in software platforms based on general purpose processors.

Mavenir vRAN OpenRAN Solutions

Mavenir has created the world's first fully containerized, virtualized OpenRAN Split 7.2 architecture. The solution provides the flexibility to deploy vRAN in a public or private cloud while supporting radios from different vendors on open interfaces.

Mavenir's award-winning vRAN OpenRAN solution provides the flexibility to support all network deployments, including private and public cloud, and multi-generational use cases in cloud-native architecture. Providers can reduce time to market with customized features using Mavenir's 100% software-based solution (see Figure 4). TCO can be optimized with reduced capex/opex resulting in a near 40% savings in five years by leveraging web-scale economics, expanded supply chains, and commercial off-the-shelf (COTS) hardware.

Figure 4.



Elimination of Proprietary and Compartmentalized Layers Running on Proprietary Hardware
Legacy Solution
Handset
Data
Radio Unit
Data Packets
Base Band Unit (BBU)
Software
Proprietary Hardware
Data Packets
Packet Gateway
Software
Proprietary Hardware
Data Packets
Session Border Controller
Software
Proprietary Hardware
Data Packets
Call Session Control Function (IMS Core)
Software
Proprietary Hardware
Packet Encapsulation / Decapsulation at Each Step of the Process Given Different Environments
MAVENIR
Handset
Data
Radio Unit
Data Packets
Base Band Unit (BBU) + Packet Gateway + Session Border Controller
MAVENIR SOFTWARE
Data Packets
Call Session Control Function (IMS Core)
MAVENIR SOFTWARE
COMMERCIAL OFF-THE-SHELF HARDWARE
Reduced Number of Environments; Reduced Number of Hops; Less Latency; Fewer Encapsulations / Decapsulations
~40% Capex Savings (Less Hardware)
~20% Opex Savings (Traffic Optimization)[1]
Optimized solution superior to closed systems to reduce costs for MNOs

Mavenir RAN Intelligent Controller (RIC)

Mavenir's RAN Intelligent Controller (RIC) helps manage multi-vendor RAN components and enables operators to proactively manage their network resources to automate processes, mitigate service degradation and maintain a high quality of experience for their subscribers. The non-RealTime (non-RT) RIC is a containerized application that uses advanced machine learning (ML) algorithms to optimize network performance and train machine learning models using long-term RAN data for dynamic and adaptive policy and control. The near-RT RIC application hosts trained AI/ML applications to infer and control O-RAN elements in near-real time and supports such functions such as traffic steering, slice SLA management, mMIMO beamforming optimization, and industry specific use cases.

OpenRAN Evolution Adding 2G/3G Across a Single Unified RAN to Support ‘Multi-G’ Radio Access

Mavenir has established a Centre of Innovation in Cambridge, United Kingdom. The Centre will focus on Mavenir’s innovative and open virtualized Multi Radio Access Technology (vMRAT) development and specifically on the integration of the 2G and 3G capabilities. These efforts provide the industry with a unique solution for MRAT OpenRAN which is completely built on virtualized architecture, fully containerized and integrates all the ‘multi-G’ cellular stacks from 2G to 5G. The solution will feature the ability to scale and utilize a single architecture to cover all mobile technologies, giving the advantage of an extremely agile and flexible configuration for even faster time to market and for remote operations of the radio access network.

Learn more

Mavenir OpenRAN Partner Ecosystem

The OpenRAN Partner Ecosystem provides more options and makes it easy for operators to deploy an innovative, flexible cloud-based OpenRAN solution. Mavenir acts as the end-to-end systems integrator simplifying the engagement for operators and creating an offering that is on par with the traditional, hardware-centric proprietary vendors. Open interfaces are in the best interest of the network operators and the overall industry. The formation of this ecosystem creates a challenger to the traditional radio vendors. Other companies are encouraged to support this effort, which will result in a game-changer, as operators continue to seek a new economic model in a world where a traditional, hardware-based approach is no longer a viable option.

Mavenir’s OpenRAN Partners

BLUE DANUBE
COMMSCOPE
DELL
facebook connectivity
FUJITSU
hp
intel
KMW
kontron
MICROELECTRONICS TECHNOLOGY INC.
台揚科技股份有限公司
NEC
SERCOMM
SUNWAVE
ace axis A
aspire Perfecting Networks
Bai Cells
Benetel
We know wireless

Mavenir OpenRAN Services

The growing momentum for OpenRAN solutions is driving the demand from mobile operators for vendors to provide an end-to-end OpenRAN service ecosystem to design, build, optimize and maintain these networks.

Mavenir's deep experience in OpenRAN technology solutions and end-to-end networks, coupled with leading partners in supply chain management, system integration, and field installation, provides customers a full complement of solutions and services. Mavenir offers seamless integration of all RAN components (Mavenir and 3rd party) with core solutions to create a complete customer network.

Mavenir's System Integration Partners

MAVENIR   Goodman Networks®   GDT

Launching Evenstar to Accelerate OpenRAN Adoption

As a founding member of the Telecom Infra Project (TIP), Mavenir works closely with the TIP community to improve the infrastructure for global networks. Together with partners Microelectronic Technology Inc. (MTI) and in collaboration with Facebook Connectivity, Mavenir has launched the Evenstar B3 RRH, which will give mobile network operators the ability to accelerate the adoption of OpenRAN technology.

The Evenstar program focuses on building general-purpose RAN reference designs for 4G/5G networks in the OpenRAN ecosystem that are aligned with 3GPP and O-RAN specifications. The RRH architecture is based on O-RAN Alliance Fronthaul specifications based on Split 7.2.

The Evenstar B3 RRH is generally available now, with plans to expand into other OpenRAN architectural elements. The Evenstar program will eventually include multiple RRH product SKUs, including FDD B3 (4T4R 4X40W).

Mavenir’s OpenRAN Solution Detail Description

Requirement for Disaggregated OpenRAN

This document describes the general Mavenir solution and details on the O-RAN benefits, hardware, software and architecture.

Mavenir offers all the necessary hardware, software, and flexible architecture to meet the needs for these use cases:

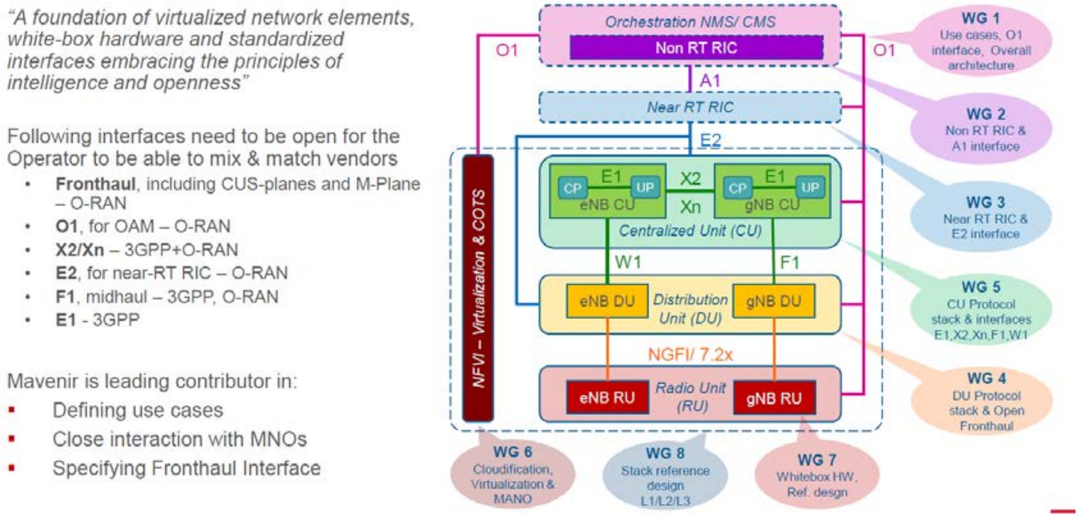
- Neutral Host Provider
- Private Networks
- Single Operator Indoor
- Outdoor capacity densification
- Outdoor Wide-Area Coverage feasibility

Mavenir RAN Solution Overview

Mavenir offers a single solution architecture addressing all the requirements on site types, functional options, and deployment types (see Figure 5). The solution has the following key characteristics:

- vRAN – fully container-based solution with IT-centric deployment techniques
- OpenRAN disaggregated architecture – fully separated CU-UP, CU-CP, DU, RU with 3GPP split 2 and ORAN 7.2x
- O-RAN standards – Mavenir fully supports standards and already supports multi-vendor commercial deployments with split 2 and split 7.2x

Figure 5.



“A foundation of virtualized network elements, white-box hardware and standardized interfaces embracing the principles of intelligence and openness”

Following interfaces need to be open for the Operator to be able to mix & match vendors

- **Fronthaul**, including CUS-planes and M-Plane – O-RAN
- **O1**, for OAM – O-RAN
- **X2/Xn** – 3GPP+O-RAN
- **E2**, for near-RT RIC – O-RAN
- **F1**, midhaul – 3GPP, O-RAN
- **E1** - 3GPP

Mavenir is leading contributor in:

- Defining use cases
- Close interaction with MNOs
- Specifying Fronthaul Interface

Orchestration NMS/ CMS
Non RT RIC
O1
O1
A1
Near RT RIC
E2
NFVI – Virtualization & COTS
CP
E1
UP
eNB CU
X2
Xn
CP
E1
UP
gNB CU
Centralized Unit (CU)
W1
F1
eNB DU
Distribution Unit (DU)
gNB DU
NGFI/ 7.2x
eNB RU
Radio Unit (RU)
gNB RU
WG 1 Use cases, O1 interface, Overall architecture
WG 2 Non RT RIC & A1 interface
WG 3 Near RT RIC & E2 interface
WG 5 CU Protocol stack & interfaces E1,X2,Xn,F1,W1
WG 4 DU Protocol stack & Open Fronthaul
WG 6 Cloudification, Virtualization & MANO
WG 8 Stack reference design L1/L2/L3
WG 7 Whitebox HW, Ref. desgn

The Mavenir O-RAN solution is 100% compliant with the O-RAN architecture standards. Mavenir completely follows the standards set by the O-RAN Alliance.

Advantages of O-RAN

The RAN has traditionally been the most capital- and operation-intensive component for Mobile Network Operators (MNO). Incumbent vendors are determined to keep access network interfaces closed, so competitors are effectively barred from this network segment. The industry finds itself with an opportunity to move toward truly OpenRAN interface standards. This direction is actively promoted by several initiatives like the TIP. Mavenir is an active member of TIP and the O-RAN forum to promote a truly OpenRAN ecosystem. Without these changes, MNOs will not be able to sustain their profit margin and cost structure as wireless network growth demands increase. Disruptive models and architectures for communication are being introduced by companies such as Mavenir to make the access network more robust and optimized by extracting maximum performance.

With increasing demands on the mobile network, the service providers are investing in small cell solutions or Macro Radio units powering existing distributed antenna systems (DAS) to help optimize and monetize the consumer and business services on mobile devices across 3G, 4G, and Wi-Fi networks. A Mavenir TCO model shows that operators, venue owners, and enterprises could all achieve a 48% decrease in combined capex and opex over five years in an in-building small cell deployment. Mavenir Small Cell solution offers self-organizing networks (SON), management, and orchestration to enable an operator to manage their network efficiently with carrier grade quality at a reduced TCO.

Key Benefits

> Lower Opex – many use cases addressed with a single, common architecture using the latest cloud-native, container-based deployment techniques

> Reduced Capex – procurement of infrastructure from open market using “off-the-shelf” (COTS) x86 hardware, and scaling in a granular fashion

> Deployment flexibility and scalability – adapting the distributed architecture to address new business segments and multi-operator use cases either with O-RAN split 2 or split 7.2x

> Future proof – free to choose new RU vendors supporting O-RAN interfaces on practically any band. Mavenir can act as integrator to support third party RUs

> 5G Ready architecture – all popular NR introduction options including SA or NSA

> Portfolio covering 2G/3G/4G/5G – please refer to section 05 “2G/3G Solutions” for the announcement of the ip.access Ltd. acquisition by Mavenir

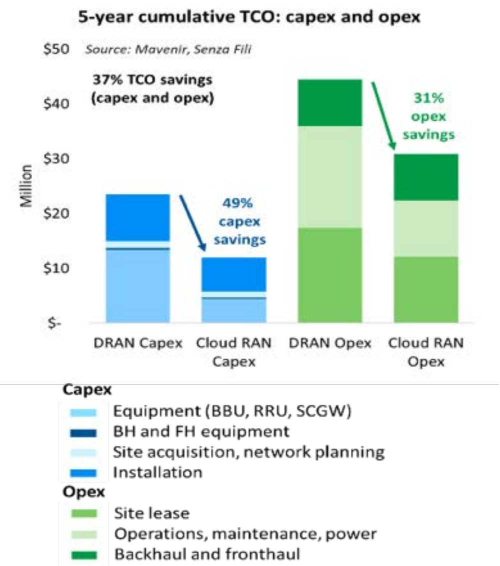
Virtualization brings one more benefit, which is easy implementation of Multi-Operator Solution (MOS). With Mavenir's MOS solution, each MNO runs all network nodes as VNFs solely dedicated to a particular MNO, while these VNFs run on shared hardware – GPP x86 COTS-based servers. Note that "VNF" refers here to virtualized or contained-based solutions.

The key drivers for network operators' interest in an OpenRAN architecture compared to proprietary solutions representing lock-in scenarios are the ability to:

> Choose for each component elements of a preferred supplier (e.g. driven by cost, feature set/best-of-breed, logistical abilities)

> Take advantage of a competitive (rather than a lock-in) environment resulting in faster technology development at lower TCO

Figure 6.



Source: Mavenir, Senza Fili

Industry analyst Senza Fili conducted an assessment that looked at several network operators defined by characteristics (number of subs, distribution of population density etc.) and compared tradition RAN deployment approaches with cloud RAN deployments.

The averaged finding for a five-year TCO showed a reduction potential of overall 37%, split into 40% capex and 31% opex (see Figure 6).

In summary, the Mavenir O-RAN approach offers the following benefits:

> COST SAVINGS. You can build a virtualized network, containerize it and each of the elements can be completely broken down. This modern network can support anywhere from tens of subscribers to millions of subscribers. It just depends on how many instances and substantiations of the VNFs and CNFs can you run on a single platform.

> MULTIPLE OPERATORS & NETWORK SHARING. OpenRAN vRAN can run multiple operators using multiple VNFs/CNFs sitting side-by-side on the same platform to create segregated networks. Another benefit is network sharing in the future through software.

> ELIMINATE VENDOR LOCK-IN. OpenRAN breaks open the interface between the remote radio head and the DU. With current vendors, it's a walled garden and proprietary. Through O-RAN, a fully open interface on Split 7.2 has been defined including all the OEM.

> 3rd PARTY TESTING BENEFITS. Radios with 3GPP specs on one side and O-RAN specs on the other will work with different vendors' baseband and because there is a defined specification with 3GPP interfaces, the elements can be tested independently. It takes pressure off operators to test in their own labs. Radios can be purchased from any vendor and tested by independently by a 3rd party and be assured that it works.

Soon radios will be produced at low cost on the basis that any operator can buy them and not get locked into a specific system integrator.

Mavenir O-RAN Architecture

Mavenir is a leading innovator in evolved, cloud-native network solutions. Mavenir is an active member of TIP and the O-RAN forum to promote a truly OpenRAN ecosystem. The Mavenir solution is based on fully open interfaces.

Mavenir RAN solution virtualizes the baseband unit, both the control plane and data plane functions, enabling the traditional BBU to be split into two independent nodes – CU (Centralized Unit) and DU (Distributed Unit). DU and CU instances can be collocated at the same site or be located separately (see Figure 7). The result is significantly higher equipment utilization, cost-efficient redundancy to achieve high availability, and lower Operation and Maintenance (O&M) costs.

Figure 7.

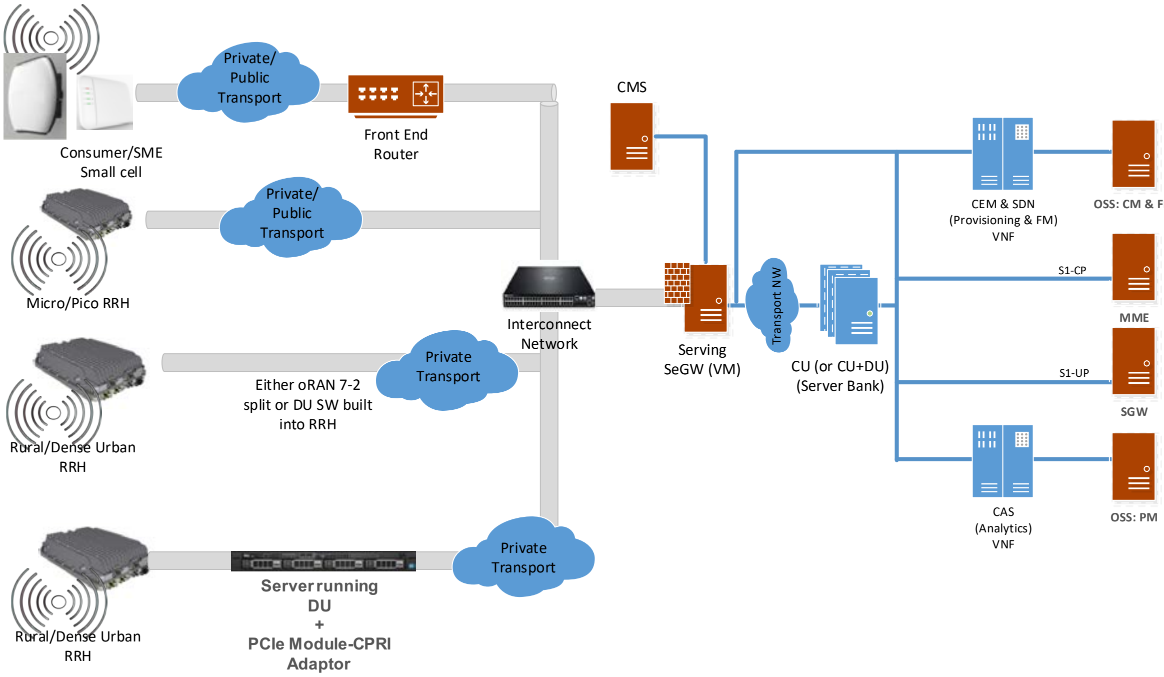
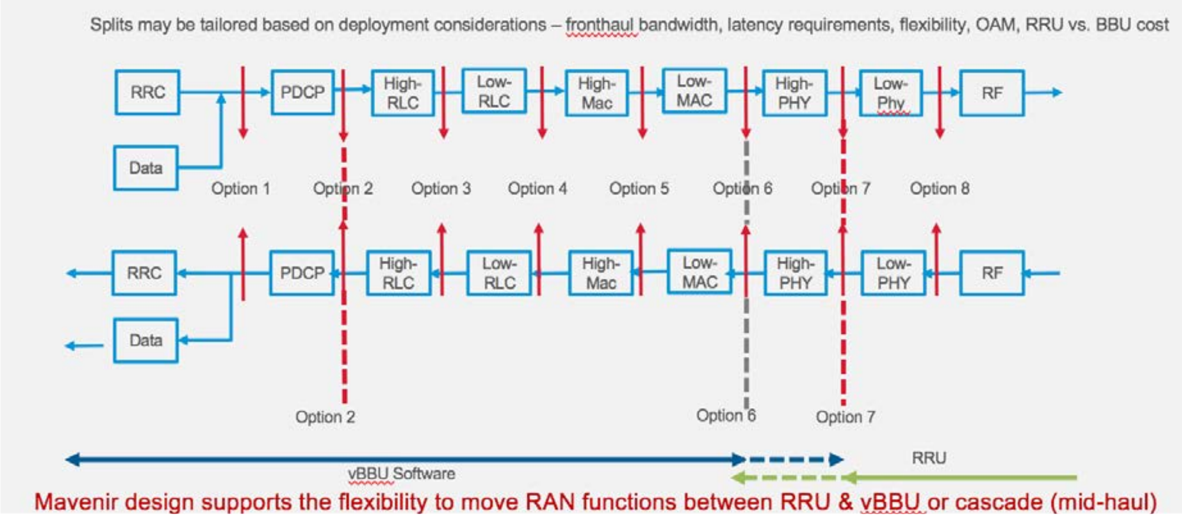


Figure 1 - Mavenir vRAN High Level Architecture

Mavenir RAN architecture supports both higher layer split (3GPP Option 2) and a lower layer split (3GPP Option 7 / ORAN 7.2 or CPRI). The low-level split allows most of the RAN, from High-PHY and above, to be virtualized (see Figure 8).

Figure 8.



Splits may be tailored based on deployment considerations – fronthaul bandwidth, latency requirements, flexibility, OAM, RRU vs. BBU cost

Mavenir design supports the flexibility to move RAN functions between RRU & vBBU or cascade (mid-haul)

Figure 2 - Functional Splits

Mavenir RAN also supports principles of Open-RAN with radio resource management (RRM) functions, such as admission control, mobility management and bearer management, disaggregated from the BBU into a common controller. The overall solution is then split into three main functional nodes:

- Remote Radio Unit (RRU) – physically provides coverage by transmitting RF signals, located at the cell site as close to antennas as possible. RRUs can also have antennas integrated in one box – Active Antenna Units (AAUs), which is the case for mMIMO RRUs and some small cell RRUs.
- Distributed Unit (DU) – controls the RLC/MAC layers, located either at the cell site or centralized at a data center (under specific conditions).
- Centralized Unit (CU) – controls the PDCP and RRC, managing several DUs and located either at the cell site (under specific conditions) or most likely at a data center.

This functionality split results in the following architectural overview from a protocol stack split perspective (see Figure 9):

Figure 9.

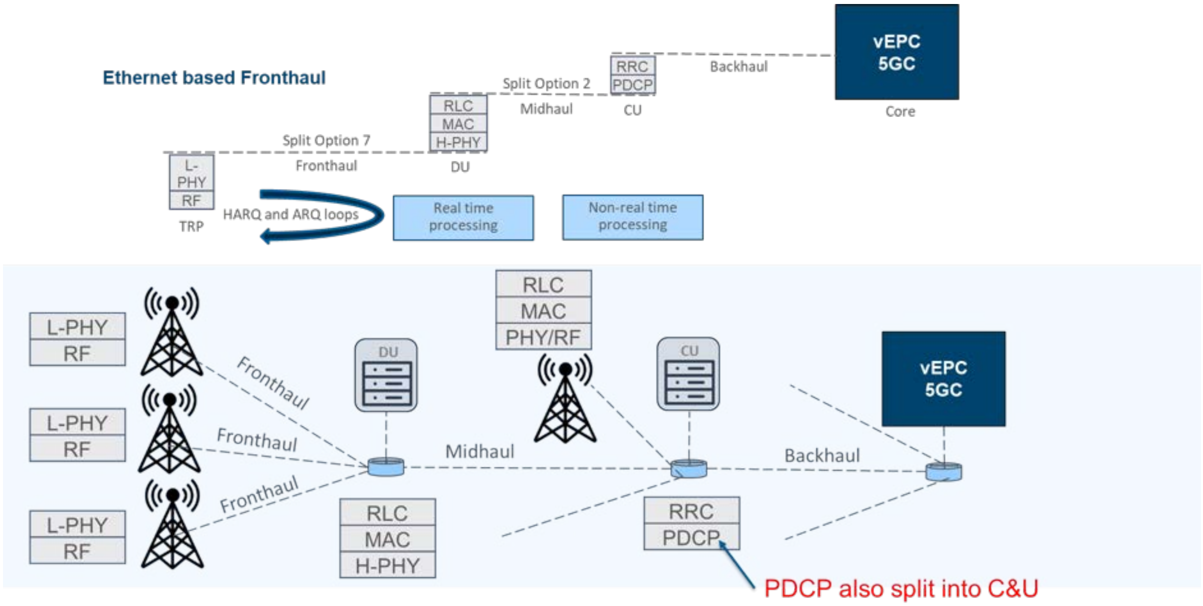
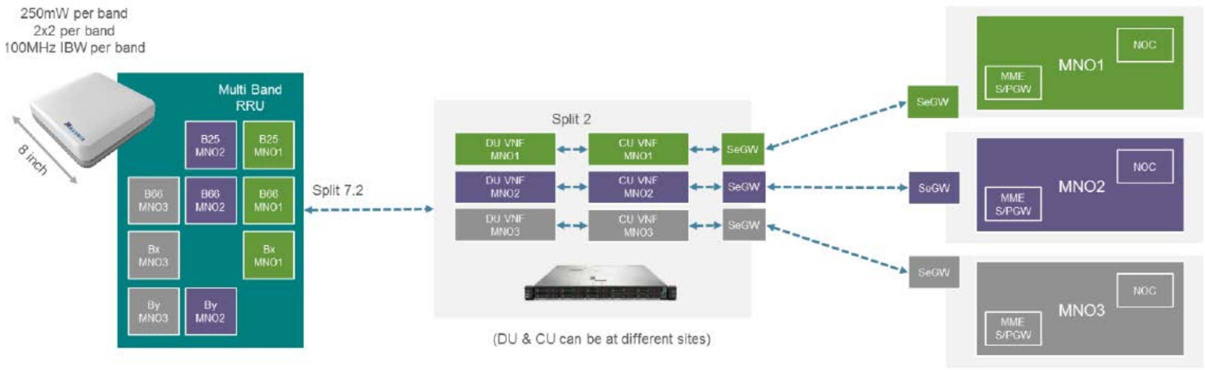


Figure 3 - Mavenir RAN High Level Architecture – protocol stack

Virtualization brings one more benefit, which is easy implementation of Multi-Operator Solution (MOS). With Mavenir's MOS solution, each MNO runs all network nodes as VNFs solely dedicated to a particular MNO, while these VNFs run on shared hardware – GPP x86 COTS-based servers (see Figure 10). Note that "VNF" refers here to virtualized or contained-based solutions.

Figure 10.



Mavenir MOS for Neutral Host

Mavenir O-RAN References

Mavenir is a leading vendor in the deployment of O-RAN solutions. Some sample public deployments are:

- VODAFONE BECOMES FIRST UK MOBILE OPERATOR TO SWITCH ON LIVE OpenRAN SITE. August 6, 2020 – Vodafone has become the first UK mobile operator to switch on a live Open Radio Access Network (OpenRAN) 4G site enabling the introduction of more suppliers for mobile networks and Mavenir is supporting Vodafone with the deployment.
- VODAFONE IDEA DEPLOYS MAVENIR OPENRAN SOLUTION. April 23, 2020 – Vodafone Idea Limited has been deployed OpenRAN on multiple Cell sites and is carrying commercial traffic since December 2019. The deployment has been carried out using Mavenir's OpenRAN solutions for 4G.
- DISH SELECTS MAVENIR TO DELIVER CLOUD-NATIVE OPENRAN SOFTWARE FOR NATION'S FIRST VIRTUAL 5G WIRELESS BROADBAND NETWORK. April 23, 2020 – As DISH Network continues its buildout of the nation's first software-defined 5G wireless broadband network, the company has entered into a multi-year agreement with leading network software provider Mavenir to deliver cloud-native OpenRAN software.
- MAVENIR AND TURKCELL PARTNER ON OpenRAN. February 27, 2020 – Mavenir has announced a business partnership with Turkcell. The two companies, together, will test and deploy OpenRAN vRAN within the Turkcell Group, initially in their home market, Turkey.

Some additional references for private networks using O-RAN technology that are also applicable to indoor coverage:

- MAVENIR AND MUGLER COLLABORATE TO DELIVER MAVENIR END-TO-END 5G PRIVATE NETWORKS IN GERMANY. February 11, 2020 – A Comprehensive Private Networks Solution for Enterprises and Industries
- NTT DATA AND MAVENIR ANNOUCE COOPERATION FOR 5G-CAMPUS NETWORKS. August 13, 2020 – Strategic cooperation to jointly develop a broad portfolio of solutions and services for private 5G and 4G networks in Germany, Switzerland, Austria.

Mavenir Solution Overview

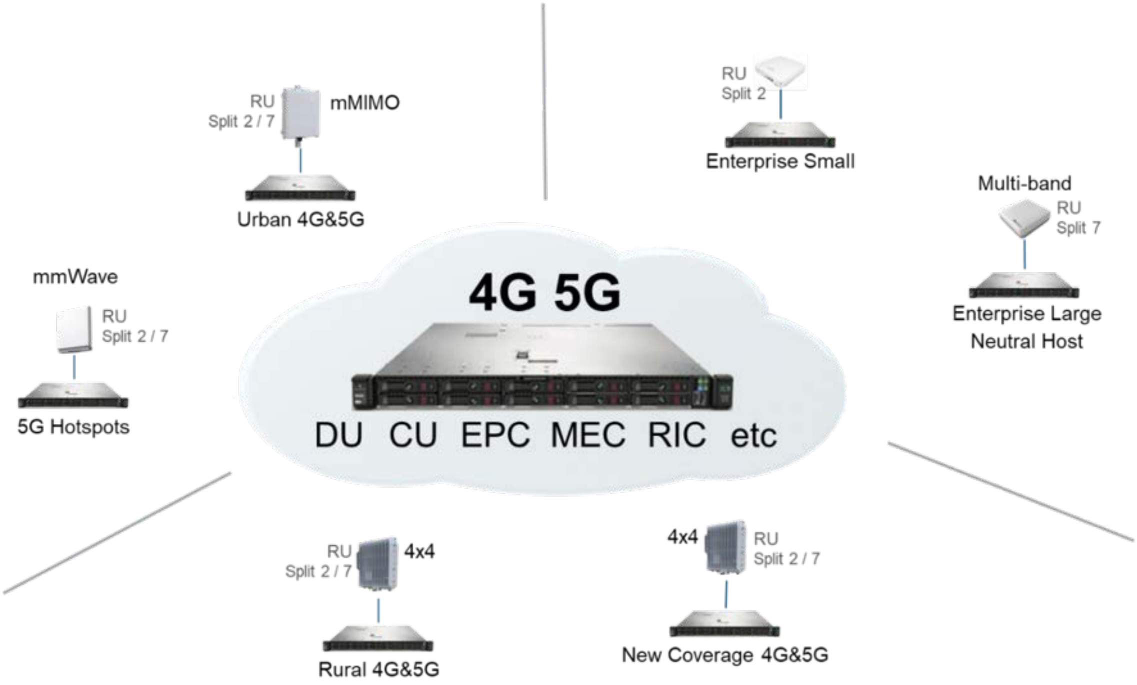
Architecture

Mavenir vRAN is based on x86 COTS hardware. This not only provides a significant lower cost-to-performance ratio but also allows making use of the much faster technology advancement cycle around COTS servers than delivered to market by proprietary, niche hardware solutions.

Mavenir vRAN supports versatility through a wide range of deployment scenarios meeting/combining various market requirements (see Figure 11), including (but not limited to):

- Deployment type (macro/small cell, outdoor/indoor)
- Radio access technology (RAT) (4G or 5G)
- Multi-band
- Time Division Duplex (TDD) or Frequency Division Duplex (FDD)
- (Massive) MIMO
- Single MNO or Neutral Host

Figure 11.



Mavenir OpenRAN – versatility

Mavenir's approach to an end-to-end solution based on open, standard-based interfaces allows Mavenir to offer one of the most versatile OpenRAN solution available on the market today.

While Figure n shows RUs based on O-RAN interfaces, Mavenir also has a CPRI converter (PCIe card-based), allowing Mavenir DU to serve also CPRI-based RUs next to O-RAN based RRUs.

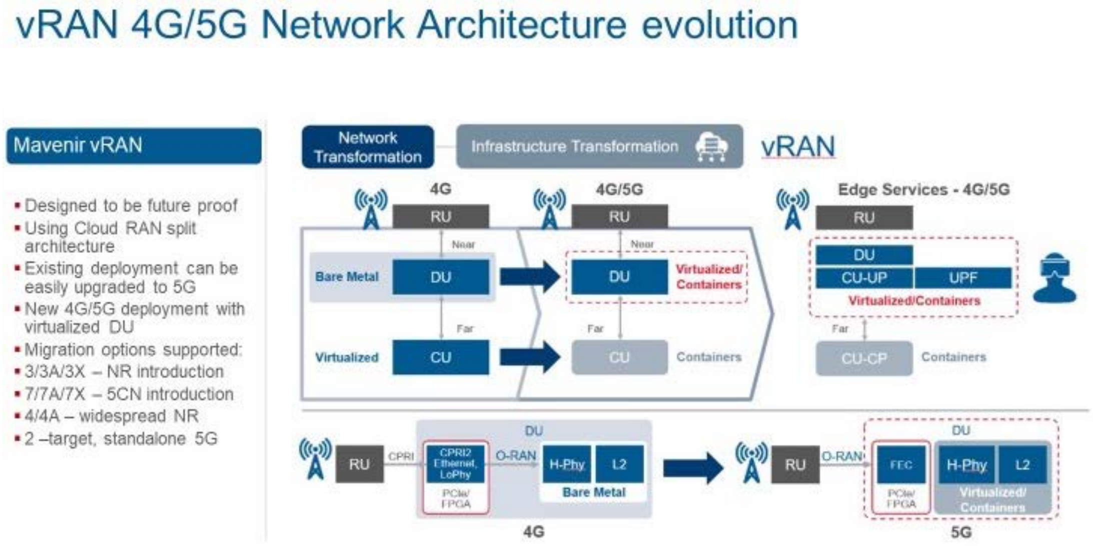
The location of the DU is driven by a number of parameters, most significantly the round-trip time (RTT) between the RU and the DU not exceeding 320μs.

Midhaul Split 2 connection between the DU and CU can be deployed on a transmission link not exceeding an RTT of 80ms, which translates to a maximum distance limit between the DU and CU of <1000km when using internet grade transmission.

4G and Non-Standalone Architecture (NSA)

The Mavenir 4G solution has been designed with 5G as a natural evolution (see Figure 12). Both 4G and 5G will be CNF-based. Although 4G was initially VNF-based, it will migrate to CNF by software upgrade only.

Figure 12.



vRAN 4G/5G Network Architecture evolution

Mavenir vRAN

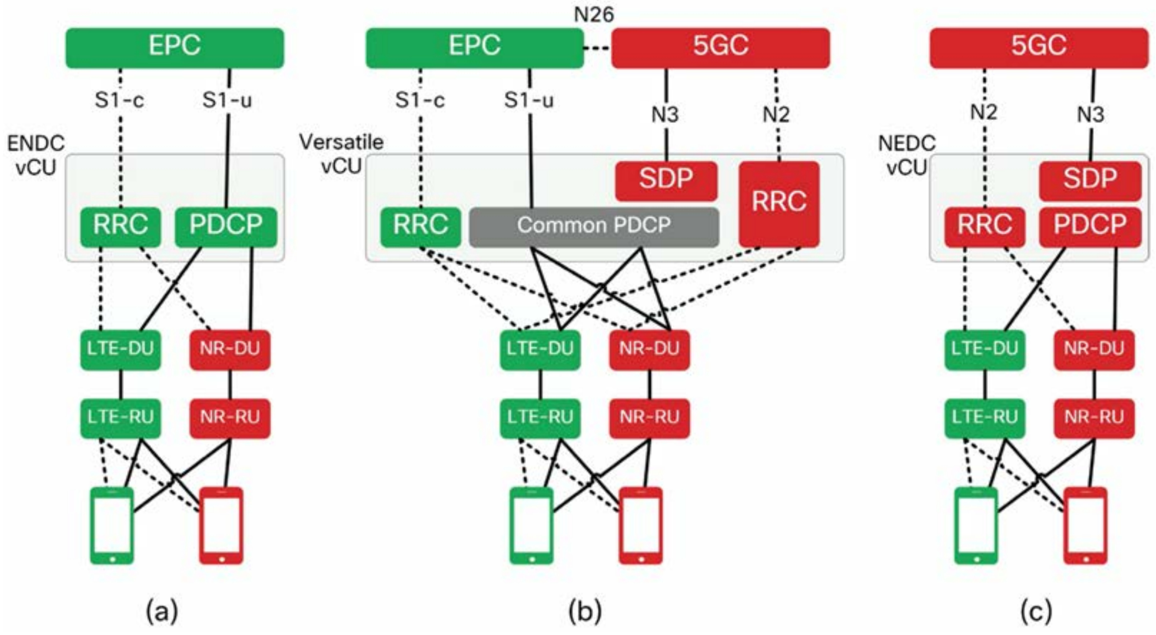
- Designed to be future proof
- Using Cloud RAN split architecture
- Existing deployment can be easily upgraded to 5G
- New 4G/5G deployment with virtualized DU
- Migration options supported:
- 3/3A/3X – NR introduction
- 7/7A/7X – 5CN introduction
- 4/4A – widespread NR
- 2 –target, standalone 5G

If required, a network operator can start with a 4G network deployment (adding NSA follows the standards approach). The architecture migration from a 4G LTE/EPC deployment to an NSA EN-DC Option 3 architecture can be performed by firstly adding EN-DC functionality and maintaining the EPC mobile core. Following that to move to Standalone (SA) a 5G Core network is required. To support devices from LTE, NSA and SA interworking between a 5GC and the EPC is required – the N26 interface (see Figure 13).

Mavenir supports E-UTRA NR Dual (EN-DC) Option 3 NSA architecture. The solution is based on standardized 3GPP and fully open O-RAN interfaces.

For a 5G EN-DC solution, NSA 3x for TDD and FDD is supported.

Figure 13.



Mavenir OpenRAN Components

CU instances are usually deployed centralized with other compute nodes (e.g., mCMS, SeGW, Plug and Play management functions) at data center locations or aggregation sites.

DU instances are usually deployed closer to the RUs (e.g., at the RU sites, at aggregation sites). DU capabilities may also be included already in the RUs themselves (in that case the RU/DU node connects directly to a CU) (see Figure 14).

Figure 14.

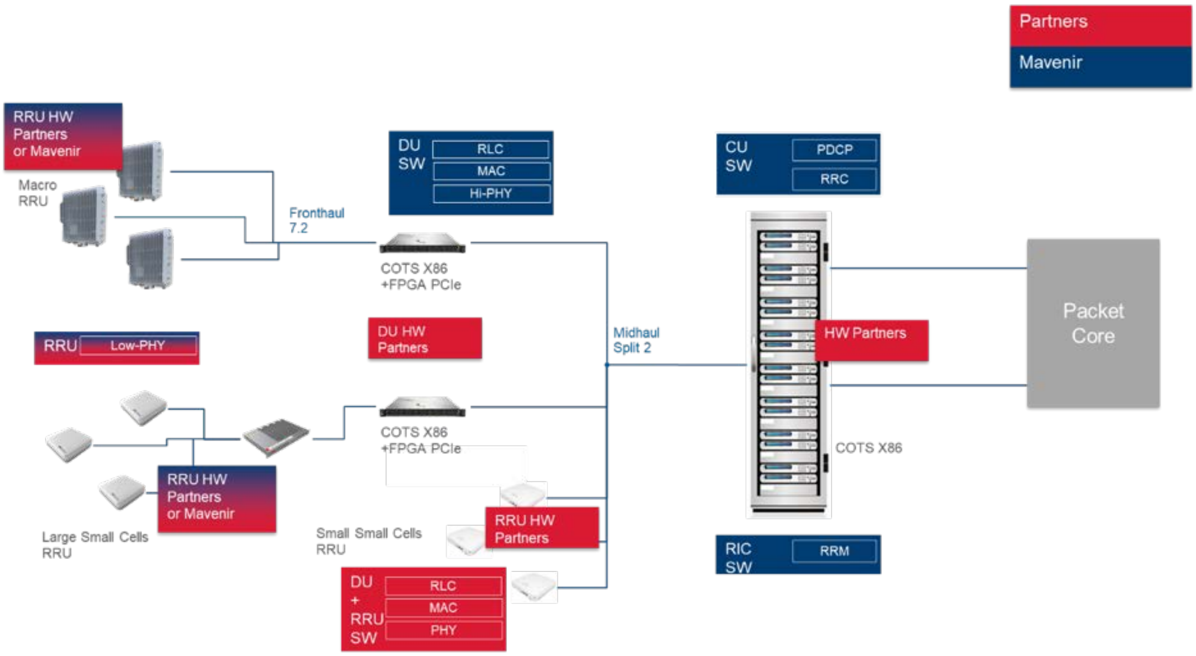


Figure 4 - Mavenir OpenRAN

The CU is fully virtualized and deployed at centralized locations or data centers. It is usually deployed as active-standby with n:m (most often 10:1) redundancy.

Mavenir Central Management System (mCMS) is fully virtualized and deployed at centralized data center locations. It is usually deployed as active-standby with 2n redundancy.

Hardware Platforms

Mavenir DU

To cover various architectural requirements, Mavenir offers DUs dedicated for both cell site and centralized (data center) deployments but can deploy on other infrastructure combinations if needed.

Mavenir CU

In most scenarios, Mavenir CU is deployed at a central data center. However, Mavenir also offers CU for cell site deployments along with DU on shared hardware. As above, Mavenir can deploy on other infrastructure combinations if needed.

Cloud Platforms

Any cloud platform which is Kubernetes-based can be used to deploy Mavenir CNF-based solutions (newest versions of eNodeB and gNodeB; for VNF-based solutions (eNodeB) RHOS or Windriver Titanium can be used). However, Mavenir offers its own platform called Mavenir Webscale Platform (MWP) which supports various types of deployments.

The Mavenir vRAN solution can be deployed in a variety of ways to suit deployment requirements. For example:

> DU deployed on bare metal on Kontron or any other servers.
> Virtualized with NFV (i.e., VNFM) in OpenStack environments.
> Fully container-based using a Container-as-a-Service/Platform-as-a-Service (CaaS/PaaS) layer (either provided by Mavenir or by the customer).

Where needed for a complete deployment, Mavenir provides the Mavenir Webscale Platform (MWP). MWP enables solutions to be deployed using Docker-based containers and relies on a Kubernetes environment for container orchestration and management. Kubernetes platform is an extensive and powerful ecosystem providing common management features for all container-based applications. Because it is considered “state of the art” for container management, Kubernetes is an optimal choice for future proof cloud-native deployments.

OAMP - Central Management System (mCMS) and Analytics

The Mavenir MWP provides a comprehensive Fault, Configuration, Accounting, Performance, Security) (FCAPS) solution that supports the operation/management of the solution. It can be integrated with classic back-office systems using protocols such as SNMP, SFTP, SSH, etc.

The Mavenir Centralized Management System (mCMS) is a centralized management platform used to manage Mavenir solutions. This includes O-RAN and other Mavenir product lines.

The mCMS provides common view and common configuration using YANG configuration models and YANG autogenerated GUI.

Integrated RAN Configuration

The vRAN approach offers the possibility to move the entire RAN subsystem to the edge of the network (see Figure 15). Mavenir offers a complete end-to-end portfolio covering RAN, packet core, applications and OSS deployed on a common container-based platform. This means a complete network can be deployed in a local customer premises using the same product as used for other use cases.

Figure 15.

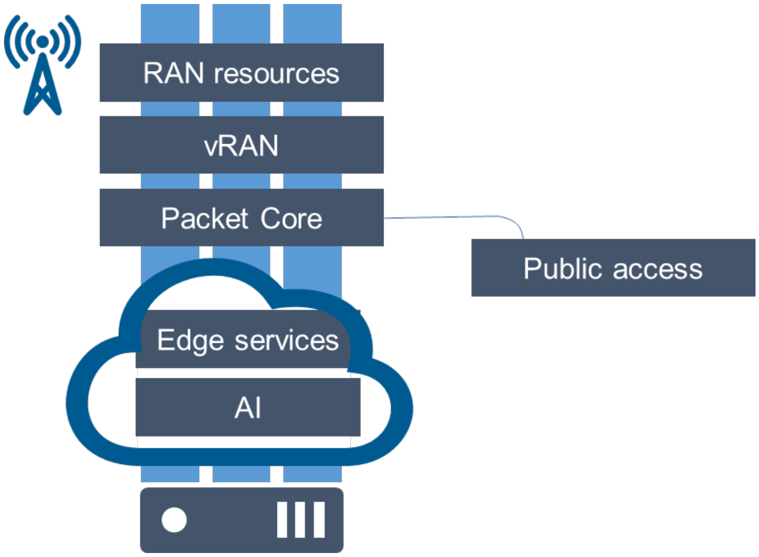


Figure 5 – Integrated solution deployment

There many use cases for this type of deployment:

- Private networks for enterprises
- Industrial use cases
- Secure networks for utilities
- Local breakout for Multi-access Edge Computing (MEC)

An important aspect of this type of deployment is zero touch provisioning (ZTP). Mavenir is developing an end-to-end solution to allow this type of deployment into many environments.

2G/3G Solutions

In September 2020, Mavenir acquired ip.access Ltd, a leading 2G, 3G, 4G and 5G-ready small cell solutions provider. This acquisition extends Mavenir's leadership in OpenRAN radio on three fronts:

- Communication Service Providers: Adding 2G and 3G capabilities to the OpenRAN portfolio
- Enterprise: Adding a full suite of enterprise radio solutions for Mavenir's Private Network offerings, including OnGo/CBRS certified solutions
- Non-traditional Networks: Leveraging market leading software defined vRAN solutions for Aviation, Maritime, Rural and Remote networks with next generation solutions in the air, on land and at sea (see Figure 16)

Figure 16.

Sample of IP Access – the Mavenir company 2G/3G/4G indoor & outdoor portfolio

RCRWireless News

INTELLIGENCE ON ALL THINGS WIRELESS

WHITE PAPER

SEPTEMBER 2020

OPENING THE RAN OPENS UP NEW EDGE OPPORTUNITIES

Dell Technologies OEM Solutions and Mavenir have a “vision to transform the cell site”

MAVENIR

DELL Technologies | intel

FOR MORE INFO PLEASE VISIT: Dell Technologies

Like many things, 5G is an exercise in scale--more network capacity, higher speeds, lower latency, new services. To deploy 5G networks at scale in the run-up to new service revenue opportunities, operators are allocating billions of capital dollars each year. Concurrently, 5G is, by design, prompting a shift to virtualized and cloud-native infrastructure instead of legacy, monolithic technology stacks. Trading out single-purpose equipment for general-purpose hardware capable of running any type of virtualized network function or compute workload is part and parcel to the vision of a flexible and autonomous network. The latest focus of virtualization efforts is the radio access network; in this push for virtualization, telecom is expanding the benefits of open, interoperable networking to an operator's single biggest capital expense – the RAN.

OPEN RAN IMPROVES NETWORK ECONOMICS AND DIVERSIFIES THE SUPPLY CHAIN

RAN disaggregation, de-coupling hardware and software, is meant to give operators the ability to pick and choose components and deploy cell sites in a modular fashion suited to the particular requirements of a site or use case. This process creates a virtuous cycle – replacing static fixtures with non-proprietary x86 hardware and bespoke software reduces capital expenses allowing smaller vendors to gain market share; a more competitive market creates a more advantageous economic environment for buyers; and heightened competition between vendors should drive innovation.

"OpenRAN is a huge opportunity—a massive one—for companies like Mavenir and Dell. It's a revolution right now in the telco world."

Abel Garcia, Business Development Manager, OEM Telecom Solutions, Dell Technologies

Today, "Nothing is really disaggregated," Mavenir's Stefano Cantarelli, executive vice president and chief marketing officer, explained to *RCR Wireless News*. "Operators need to go to the same supplier for all the digital and analog radio parts and the software needs to also come from the same supplier. With Open RAN, we're opening up the radio system by having open interfaces so that a remote radio unit vendor can actually be different from the baseband software vendor."

The O-RAN Alliance, an industry consortium created by major global operators, is the forum for creating open, interoperable radio interfaces. The O-RAN Alliance follows two primary principles, openness and intelligence, in its effort "to clearly define requirements and help build a supply chain ecosystem to realize its objectives" of creating "multi-vendor, interoperable, autonomous RAN."

With an Open RAN architecture, open radio interfaces are key. At a high level, operators can use a functional split architecture where a centralized unit, distributed unit and radio unit can be provided by multiple hardware and software vendors. Splitting up functionality, both in terms of where equipment is located and where specific network functions are performed, brings a new level of flexibility — a term synonymous with 5G — in terms of resource coordination, managing shifting network load, and performance optimization based on real-time, closed-loop analytics.

To understand the total cost of ownership benefits that come with vRAN, ACG Research considered the hypothetical lifecycle of a Tier 1 4G RAN supporting 10,000 subscribers from 12,000 radio sites over five years. In calculating TCO, they found that capex for a traditional RAN was twice the cost – largely attributed to a higher number of more expensive radio sites in the legacy model. For the opex side, ACG found a traditional approach is materially higher given costs for sites, fiber leasing, power and maintenance. A network-wide virtualized RAN architecture can lower TCO by up to 44% compared to a traditional RAN, according to the white paper. In a growth-focused model wherein only new sites follow a vRAN design, ACG Research found a TCO reduction of 27%.

Our findings clearly indicate that distributed virtual infrastructures for CSPs will benefit materially from the use of elastic, horizontal cloud designs.

In addition to creating more favorable network economics for operators and fostering a more competitive, diversified vendor ecosystem, distributing x86 hardware throughout a network out to radio sites opens up a number of other opportunities that are closely aligned with the vision of 5G support for real-time applications and all types of network slicing.

"5G is not only a new radio technology, it's also the promise of a new set of applications. We are creating a disaggregation between the technical infrastructure and the business models of the applications for the consumer market, the enterprise and the smart devices.."

Alexis Debreu, Telecom Architect, Dell Technologies

Vodafone turns up first live Open RAN site in the UK

In early August, multinational service provider Vodafone turned on the first Open RAN cell site in the United Kingdom. The 4G site, located at the Royal Welsh Showground agricultural facility, comprises a distributed unit and remote radio unit at the site in Wales that is connected to a centralized unit located in London and running on Dell hardware. The system uses Mavenir's vRAN software.

According to Vodafone, it will now look for additional locations to deploy Open RAN with an eye on "economically" enhancing service capabilities. Vodafone UK Chief Technology Officer Scott Petty called the activation "an important milestone. This new approach has the ability to make us less dependent on current larger technology suppliers, and find ways to reduce the cost of rolling out mobile coverage. Open RAN can also help close the digital divide between urban and rural Britain."

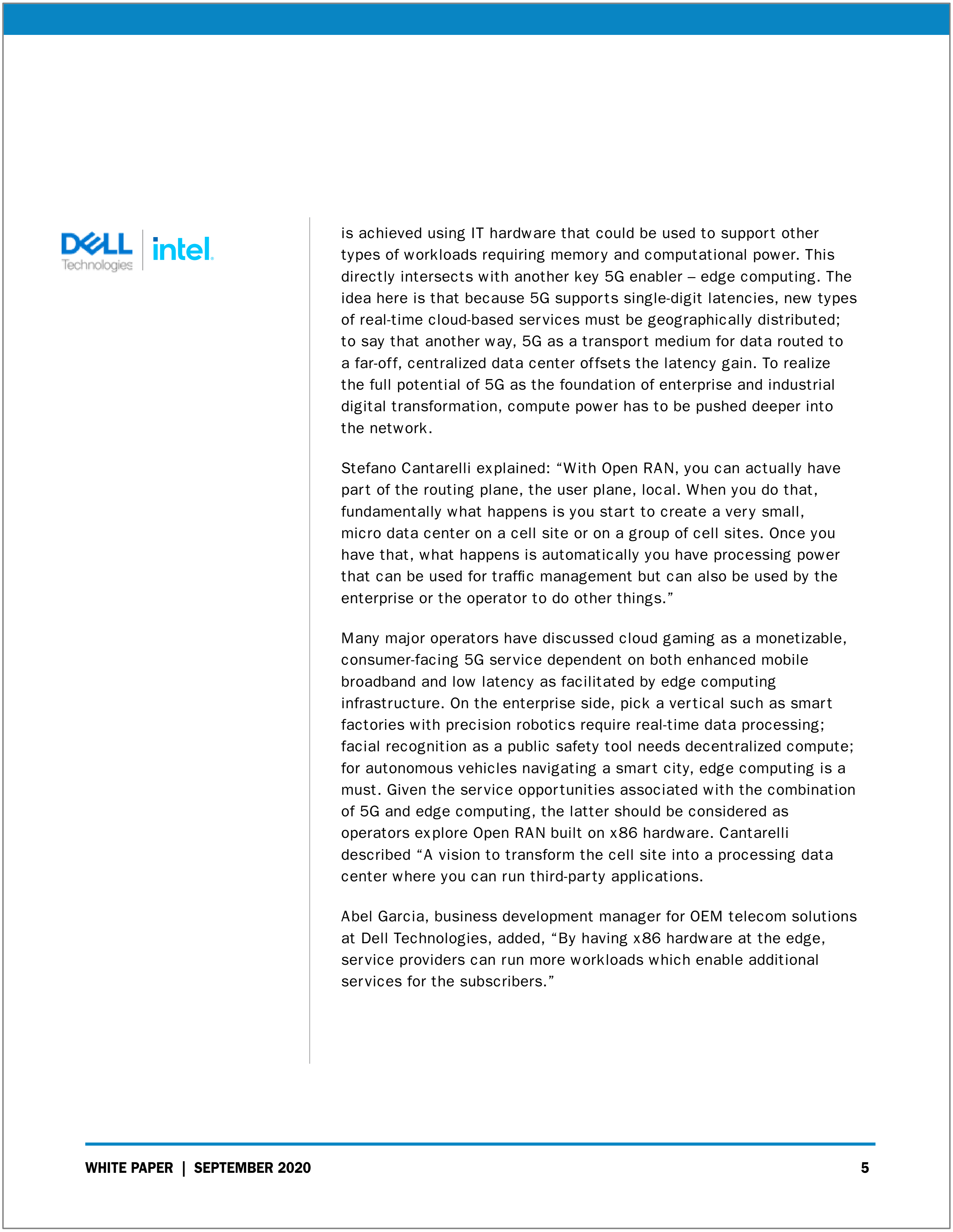
Image courtesy of Vodafone

The idea of using Open RAN to create network economics conducive to rural expansion and closing the digital divide is just part of Vodafone's interest in the technology. In addition to its work in the U.K., the operator has tested Open RAN in rural parts of Mozambique, Democratic Republic of Congo and Turkey. But Voda's Open RAN plans are more expansive. During a July call with industry analysts, CEO Nick Read said, "We think we'll have a rural Open RAN ready for 2021 and we are looking to an urban, which is a more complex execution, in 2022."

In fact, last year Vodafone announced it will include Open RAN vendors in a tender covering its entire European footprint. Speaking in November at the Telecom Infra Project Summit in Amsterdam, Head of Network Strategy and Architecture Yago Tenorio said, "Right now this is the biggest tender in this industry in the world. It's a really big opportunity for Open RAN to scale…Our ambition is to have modern, up to date, lower-cost kit in every site."

DISTRIBUTED, VIRTUALIZED INFRASTRUCTURE ENABLES AGILE SERVICE CAPABILITIES

Open RAN, similar to the cloud-native 5G core for standalone networks, uses x86 non-proprietary hardware running virtualized network functions. In other words, this highly specialized functionality



is achieved using IT hardware that could be used to support other types of workloads requiring memory and computational power. This directly intersects with another key 5G enabler – edge computing. The idea here is that because 5G supports single-digit latencies, new types of real-time cloud-based services must be geographically distributed; to say that another way, 5G as a transport medium for data routed to a far-off, centralized data center offsets the latency gain. To realize the full potential of 5G as the foundation of enterprise and industrial digital transformation, compute power has to be pushed deeper into the network.

Stefano Cantarelli explained: “With Open RAN, you can actually have part of the routing plane, the user plane, local. When you do that, fundamentally what happens is you start to create a very small, micro data center on a cell site or on a group of cell sites. Once you have that, what happens is automatically you have processing power that can be used for traffic management but can also be used by the enterprise or the operator to do other things.”

Many major operators have discussed cloud gaming as a monetizable, consumer-facing 5G service dependent on both enhanced mobile broadband and low latency as facilitated by edge computing infrastructure. On the enterprise side, pick a vertical such as smart factories with precision robotics require real-time data processing; facial recognition as a public safety tool needs decentralized compute; for autonomous vehicles navigating a smart city, edge computing is a must. Given the service opportunities associated with the combination of 5G and edge computing, the latter should be considered as operators explore Open RAN built on x86 hardware. Cantarelli described “A vision to transform the cell site into a processing data center where you can run third-party applications.

Abel Garcia, business development manager for OEM telecom solutions at Dell Technologies, added, “By having x86 hardware at the edge, service providers can run more workloads which enable additional services for the subscribers.”

Prepare your network for 5G now with Dell Technologies OEM Solutions and Mavenir

The fundamental appeal of 5G lies in the fact that the entire infrastructure acts as a cohesive platform for innovative applications and is tuned to flex with demand – providing services tailored to unique characteristics. This smart network infrastructure and an enhanced ability to support exponential scale for connectivity opens the doors to innovative applications across a variety of markets, including smart cities and manufacturing and connected healthcare and agriculture. Mavenir is committed to cloud-centric infrastructure across its end-to-end 5G portfolio (vRAN, vEPC, IMS, security, and other critical solutions), using open development techniques and programming tools to deliver the networks of the future.

Mavenir's Mobile 5G Network in a Box is an Open RAN-based vRAN, vEPC and IMS core, with all mobile network elements located on a very small number of servers in a single enclosure. The **Mobile 5G Network in a Box** provides a number of important capabilities:

- Enables 5G network slicing
- Split 2 architecture with Sercomm DU
- Split 7-2 architecture with MTI remote radio head
- Auto-provisioned CU through CEM Orchestrator

The **Mobile Network in a Box** demonstrates innovative, open interfaces, cloud-based architectures and virtualized solutions that are reinvigorating innovation outside of the traditional NEPs to the benefit of CSPs and the overall industry. The Open RAN approach frees operators from lock-in with incumbent infrastructure, making it easier to deploy a cloud-based Open RAN solution.

(cont'd on following page)

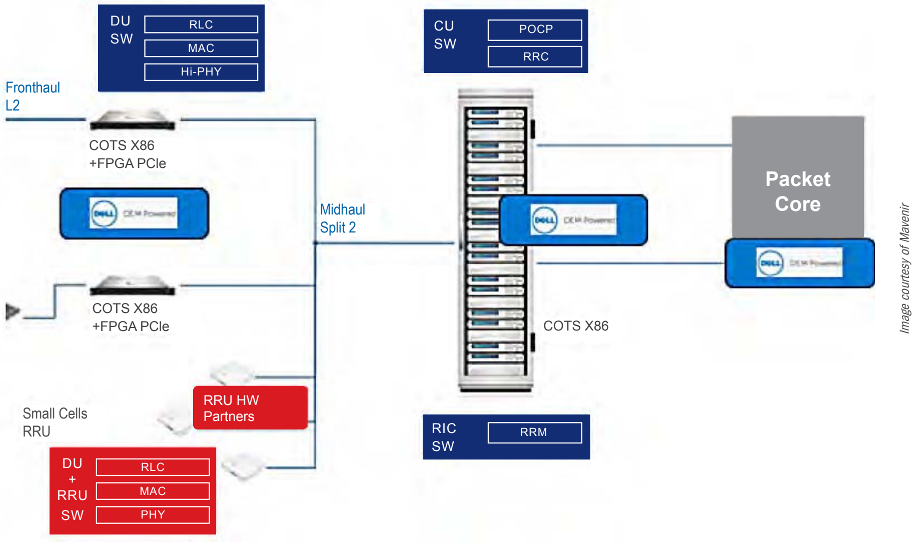


Image courtesy of Mavenir

Prepare your network for 5G now with Dell Technologies OEM Solutions and Mavenir *(cont'd)*

Telco organizations can't afford to compromise service speed and agility—they need strong infrastructure performance, robust security and reliable solutions that can scale to meet regional and worldwide demands. Dell Technologies provides the infrastructure and partnership that telcos need to focus on deploying and expanding their services.

Service providers and NEPs build for success with PowerEdge carrier-grade servers that are NEBS Level 3 and ETSI validated. The Dell EMC PowerEdge XE2420 demonstrates an ongoing evolution from the core to the cloud to the edge, leveraging the capabilities of Intel® Xeon® Scalable processors as telcos transform their networks and prepare for the 5G revolution. The combination of these two technologies provides a powerful edge platform from which telcos can deliver applications (such as vCDN and vRAN) while providing the foundation for new 5G-based enterprise services to industries such as healthcare and manufacturing.

Image courtesy of Dell

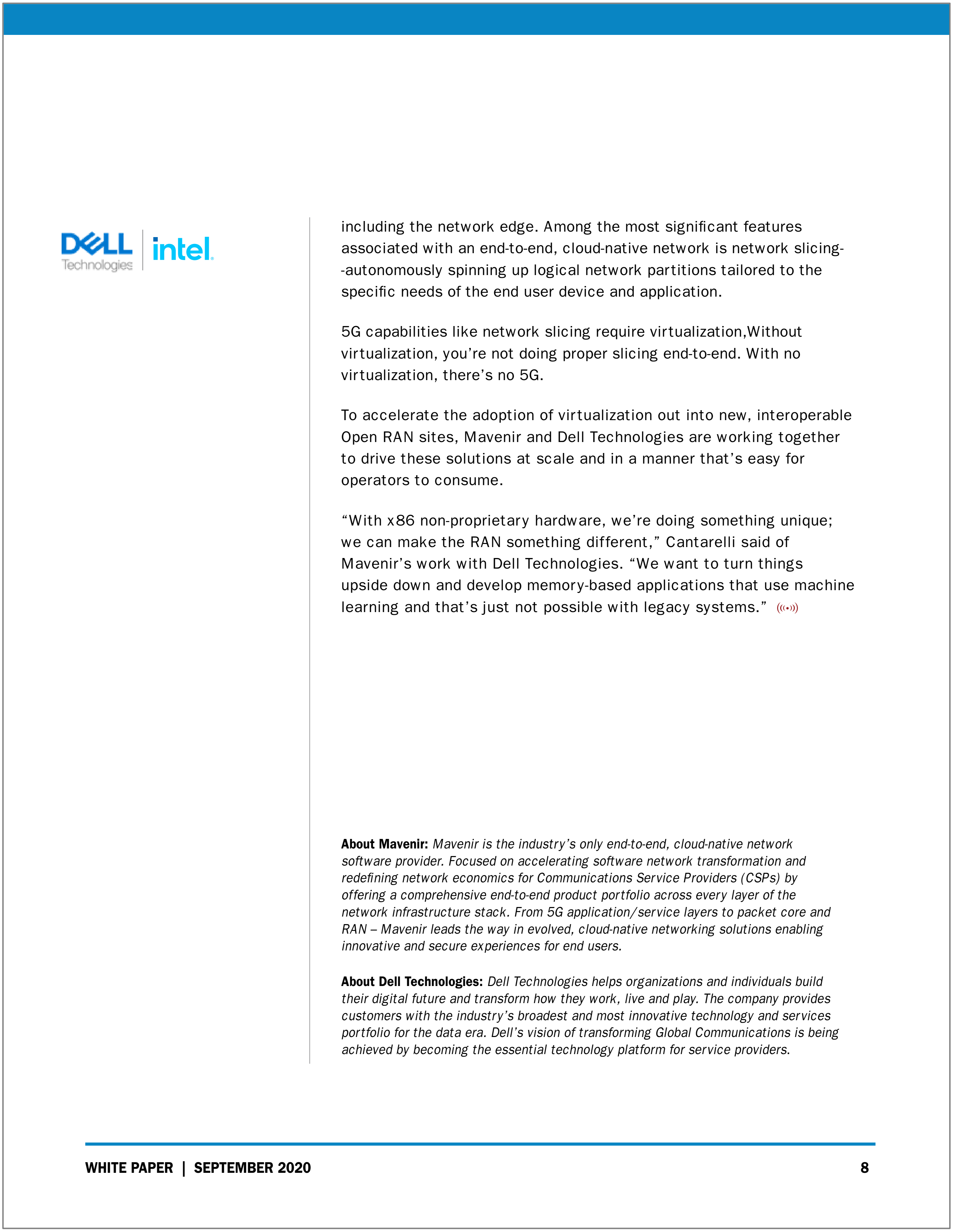
Dell Technologies OEM Solutions has 25 years of domain and industry expertise working with telecom frontrunners to solve the toughest tech challenges across all phases of product development—from architecture to integration. Partnering with Dell Technologies Solutions enables network equipment providers to elevate applications and workload performance with carrier-grade, software-defined infrastructure which are built, configured, tested and optimized to fit exact workloads, scale and environmental regulations.

"The fact that Dell Technologies is among the most established partners is important. We can build together ready to deploy and versatile solutions at scale."

Stefano Cantarelli, Executive Vice President and Chief Marketing Officer, Mavenir

WITH NO VIRTUALIZATION, THERE'S NO 5G

Open RAN, similar to the cloud-native 5G core for standalone Virtualization of core network functions has had a major impact on telecom networks in terms of cost, operation, management and capabilities. As 5G brings about a shift to cloud-native core architecture and an extension of virtualization from the core out to the RAN and



including the network edge. Among the most significant features associated with an end-to-end, cloud-native network is network slicing--autonomously spinning up logical network partitions tailored to the specific needs of the end user device and application.

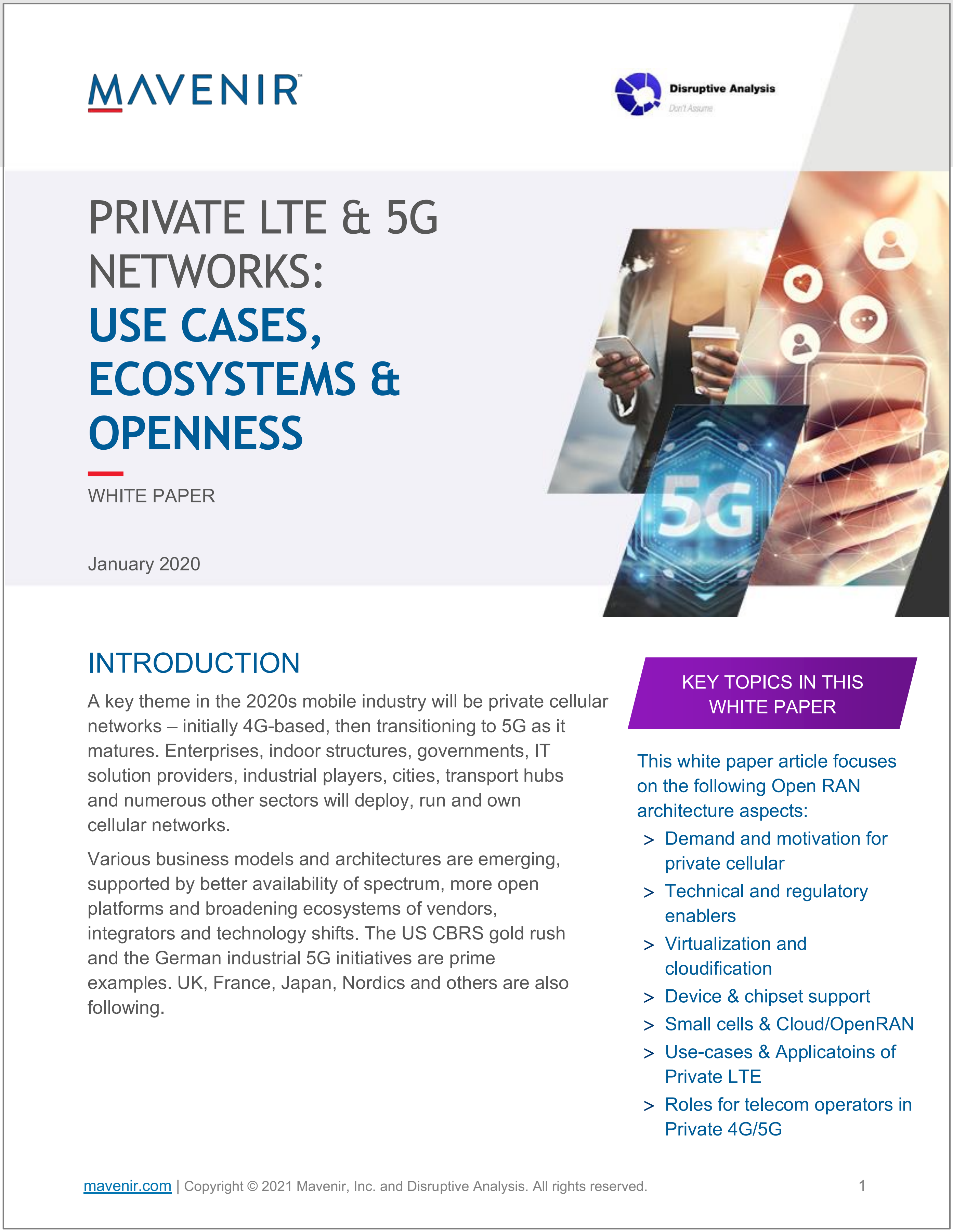
5G capabilities like network slicing require virtualization,Without virtualization, you're not doing proper slicing end-to-end. With no virtualization, there's no 5G.

To accelerate the adoption of virtualization out into new, interoperable Open RAN sites, Mavenir and Dell Technologies are working together to drive these solutions at scale and in a manner that's easy for operators to consume.

"With x86 non-proprietary hardware, we're doing something unique; we can make the RAN something different," Cantarelli said of Mavenir's work with Dell Technologies. "We want to turn things upside down and develop memory-based applications that use machine learning and that's just not possible with legacy systems." ((•))

About Mavenir: *Mavenir is the industry's only end-to-end, cloud-native network software provider. Focused on accelerating software network transformation and redefining network economics for Communications Service Providers (CSPs) by offering a comprehensive end-to-end product portfolio across every layer of the network infrastructure stack. From 5G application/service layers to packet core and RAN – Mavenir leads the way in evolved, cloud-native networking solutions enabling innovative and secure experiences for end users.*

About Dell Technologies: *Dell Technologies helps organizations and individuals build their digital future and transform how they work, live and play. The company provides customers with the industry's broadest and most innovative technology and services portfolio for the data era. Dell's vision of transforming Global Communications is being achieved by becoming the essential technology platform for service providers.*



PRIVATE LTE & 5G NETWORKS: USE CASES, ECOSYSTEMS & OPENNESS

WHITE PAPER

January 2020

INTRODUCTION

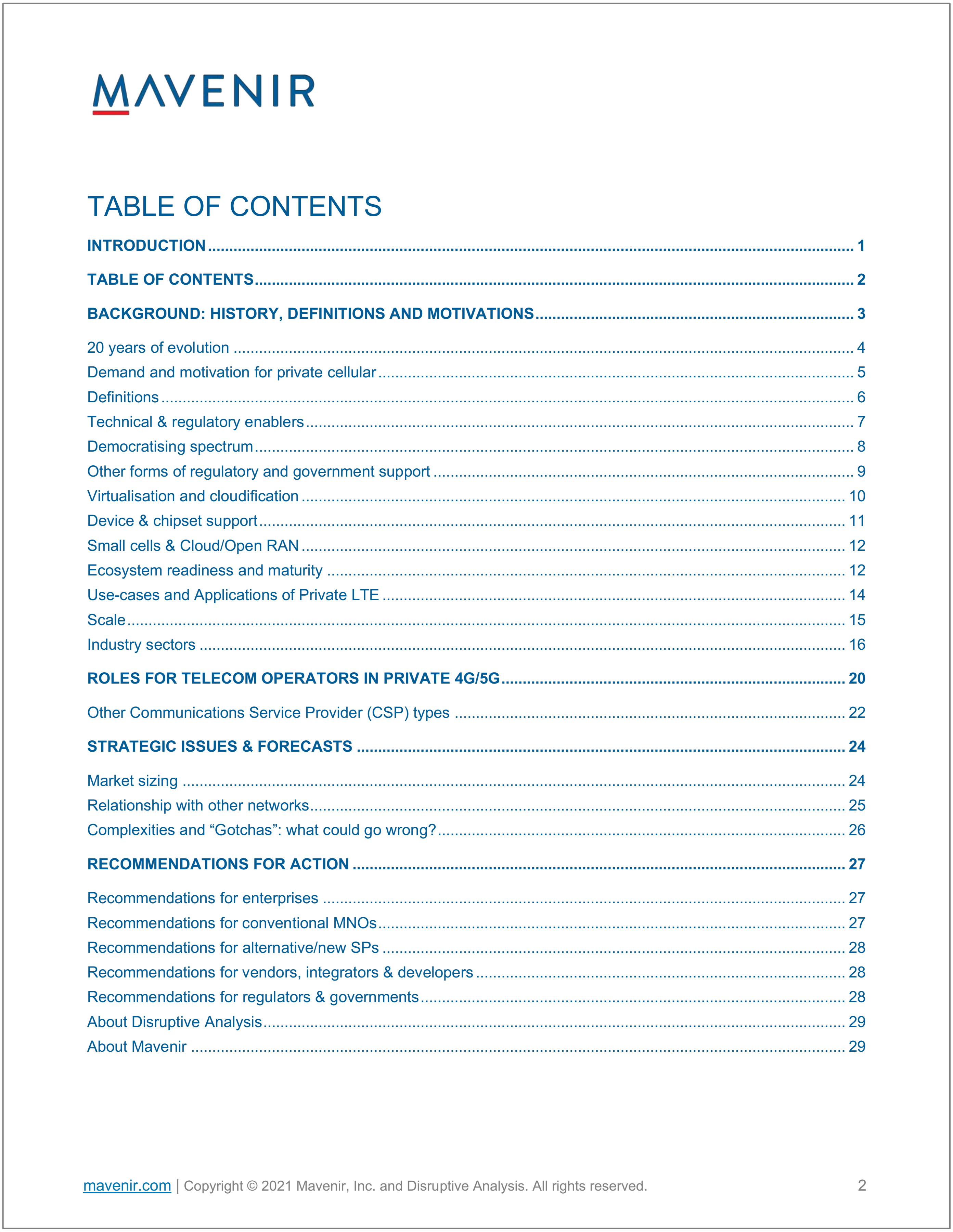
A key theme in the 2020s mobile industry will be private cellular networks – initially 4G-based, then transitioning to 5G as it matures. Enterprises, indoor structures, governments, IT solution providers, industrial players, cities, transport hubs and numerous other sectors will deploy, run and own cellular networks.

Various business models and architectures are emerging, supported by better availability of spectrum, more open platforms and broadening ecosystems of vendors, integrators and technology shifts. The US CBRS gold rush and the German industrial 5G initiatives are prime examples. UK, France, Japan, Nordics and others are also following.

KEY TOPICS IN THIS WHITE PAPER

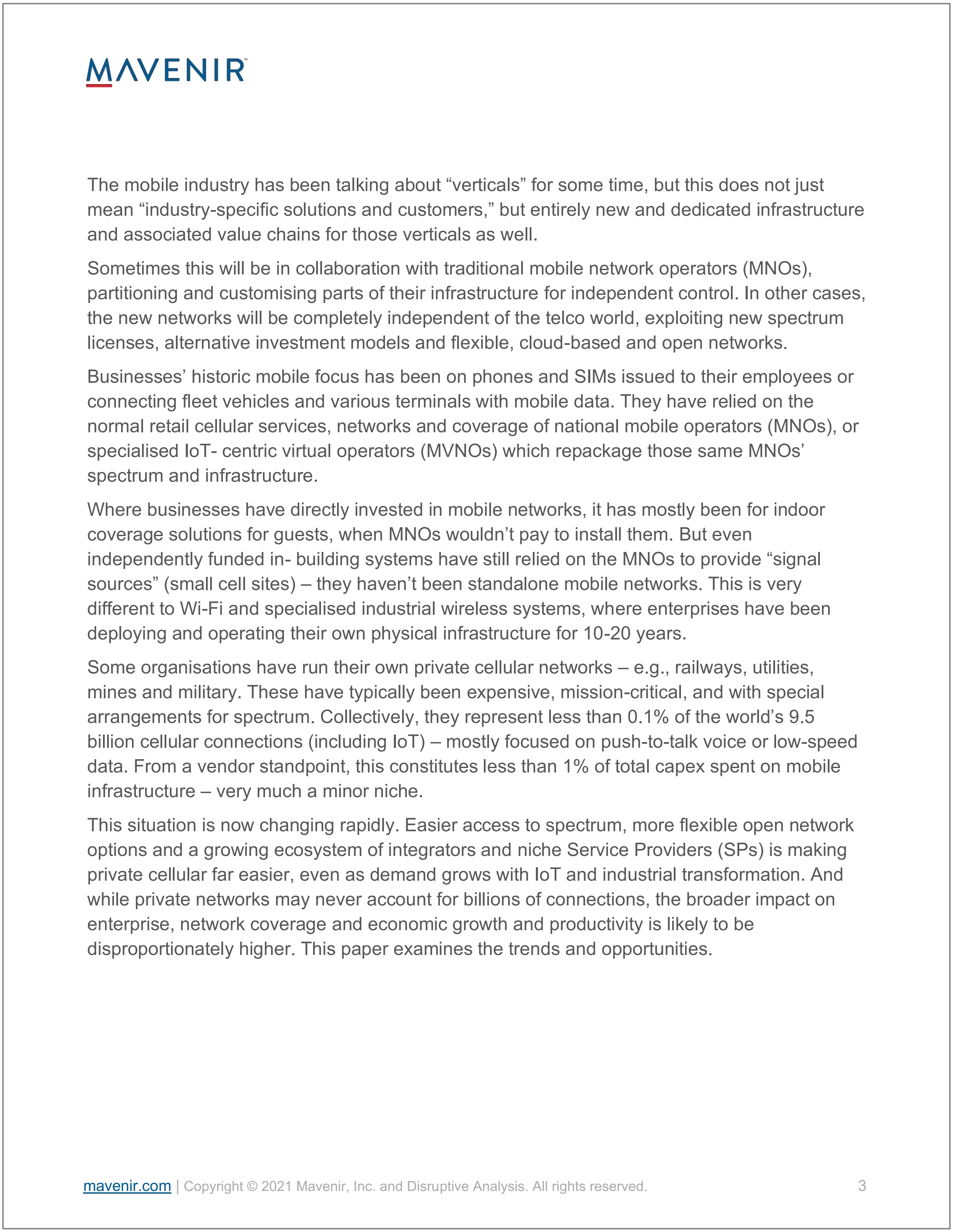
This white paper article focuses on the following Open RAN architecture aspects:

- > Demand and motivation for private cellular
- > Technical and regulatory enablers
- > Virtualization and cloudification
- > Device & chipset support
- > Small cells & Cloud/OpenRAN
- > Use-cases & Applicatoins of Private LTE
- > Roles for telecom operators in Private 4G/5G



MAVENIR

TABLE OF CONTENTS



The mobile industry has been talking about "verticals" for some time, but this does not just mean "industry-specific solutions and customers," but entirely new and dedicated infrastructure and associated value chains for those verticals as well.

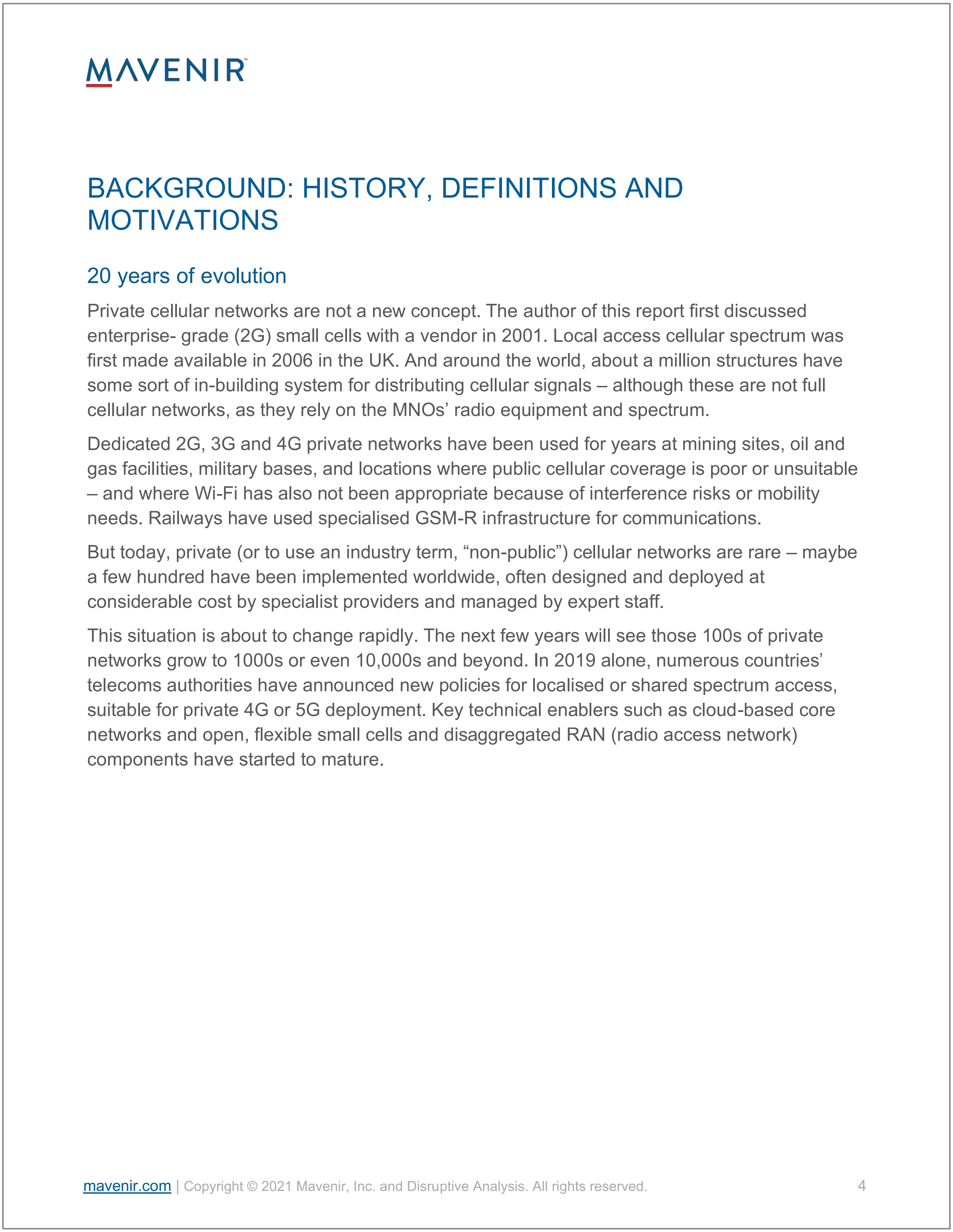
Sometimes this will be in collaboration with traditional mobile network operators (MNOs), partitioning and customising parts of their infrastructure for independent control. In other cases, the new networks will be completely independent of the telco world, exploiting new spectrum licenses, alternative investment models and flexible, cloud-based and open networks.

Businesses' historic mobile focus has been on phones and SIMs issued to their employees or connecting fleet vehicles and various terminals with mobile data. They have relied on the normal retail cellular services, networks and coverage of national mobile operators (MNOs), or specialised IoT- centric virtual operators (MVNOs) which repackage those same MNOs' spectrum and infrastructure.

Where businesses have directly invested in mobile networks, it has mostly been for indoor coverage solutions for guests, when MNOs wouldn't pay to install them. But even independently funded in- building systems have still relied on the MNOs to provide "signal sources" (small cell sites) – they haven't been standalone mobile networks. This is very different to Wi-Fi and specialised industrial wireless systems, where enterprises have been deploying and operating their own physical infrastructure for 10-20 years.

Some organisations have run their own private cellular networks – e.g., railways, utilities, mines and military. These have typically been expensive, mission-critical, and with special arrangements for spectrum. Collectively, they represent less than 0.1% of the world's 9.5 billion cellular connections (including IoT) – mostly focused on push-to-talk voice or low-speed data. From a vendor standpoint, this constitutes less than 1% of total capex spent on mobile infrastructure – very much a minor niche.

This situation is now changing rapidly. Easier access to spectrum, more flexible open network options and a growing ecosystem of integrators and niche Service Providers (SPs) is making private cellular far easier, even as demand grows with IoT and industrial transformation. And while private networks may never account for billions of connections, the broader impact on enterprise, network coverage and economic growth and productivity is likely to be disproportionately higher. This paper examines the trends and opportunities.



BACKGROUND: HISTORY, DEFINITIONS AND MOTIVATIONS

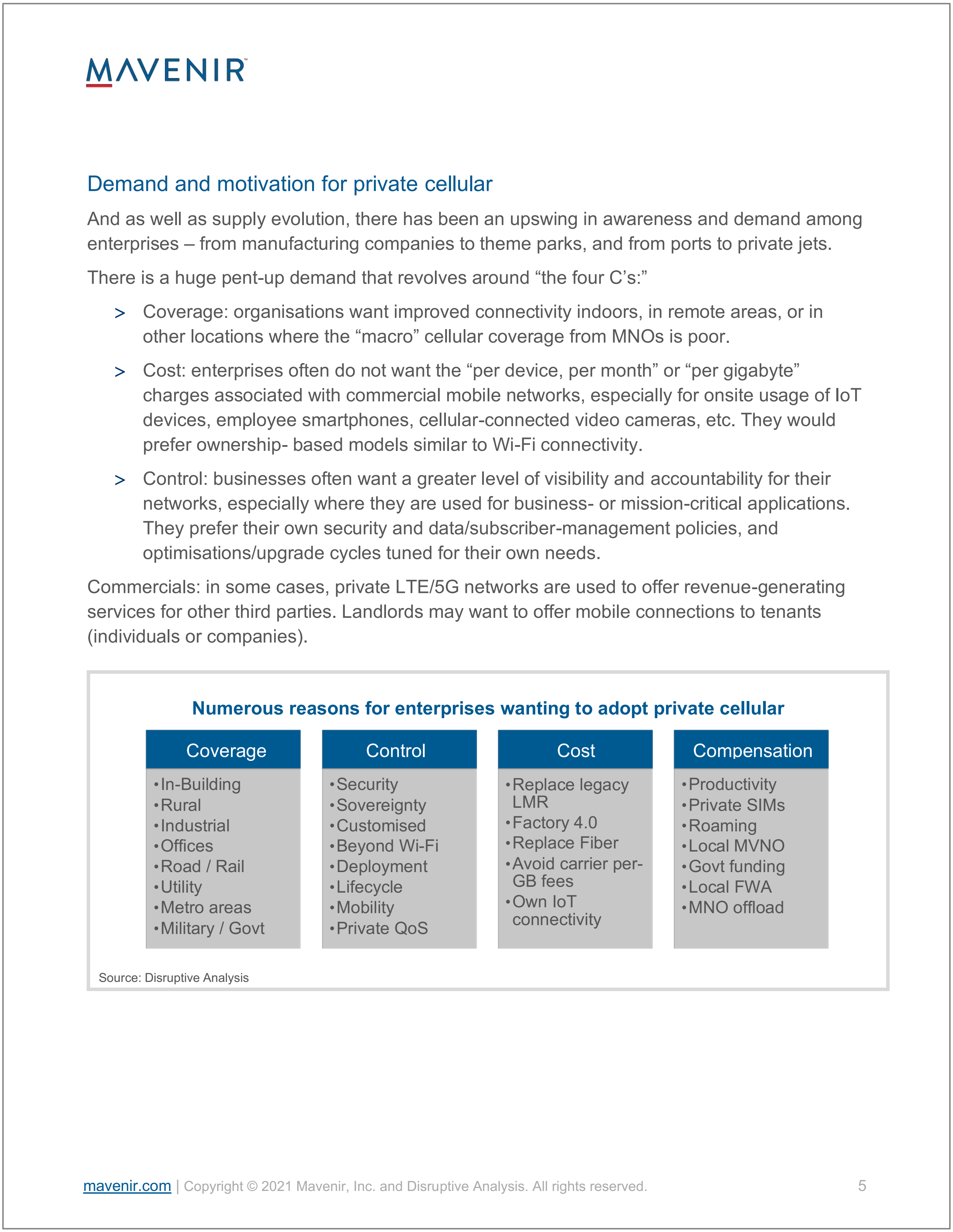
20 years of evolution

Private cellular networks are not a new concept. The author of this report first discussed enterprise- grade (2G) small cells with a vendor in 2001. Local access cellular spectrum was first made available in 2006 in the UK. And around the world, about a million structures have some sort of in-building system for distributing cellular signals – although these are not full cellular networks, as they rely on the MNOs' radio equipment and spectrum.

Dedicated 2G, 3G and 4G private networks have been used for years at mining sites, oil and gas facilities, military bases, and locations where public cellular coverage is poor or unsuitable – and where Wi-Fi has also not been appropriate because of interference risks or mobility needs. Railways have used specialised GSM-R infrastructure for communications.

But today, private (or to use an industry term, "non-public") cellular networks are rare – maybe a few hundred have been implemented worldwide, often designed and deployed at considerable cost by specialist providers and managed by expert staff.

This situation is about to change rapidly. The next few years will see those 100s of private networks grow to 1000s or even 10,000s and beyond. In 2019 alone, numerous countries' telecoms authorities have announced new policies for localised or shared spectrum access, suitable for private 4G or 5G deployment. Key technical enablers such as cloud-based core networks and open, flexible small cells and disaggregated RAN (radio access network) components have started to mature.



MAVENIR

Demand and motivation for private cellular

And as well as supply evolution, there has been an upswing in awareness and demand among enterprises – from manufacturing companies to theme parks, and from ports to private jets.

There is a huge pent-up demand that revolves around “the four C’s:”

> Coverage: organisations want improved connectivity indoors, in remote areas, or in other locations where the “macro” cellular coverage from MNOs is poor.

> Cost: enterprises often do not want the “per device, per month” or “per gigabyte” charges associated with commercial mobile networks, especially for onsite usage of IoT devices, employee smartphones, cellular-connected video cameras, etc. They would prefer ownership- based models similar to Wi-Fi connectivity.

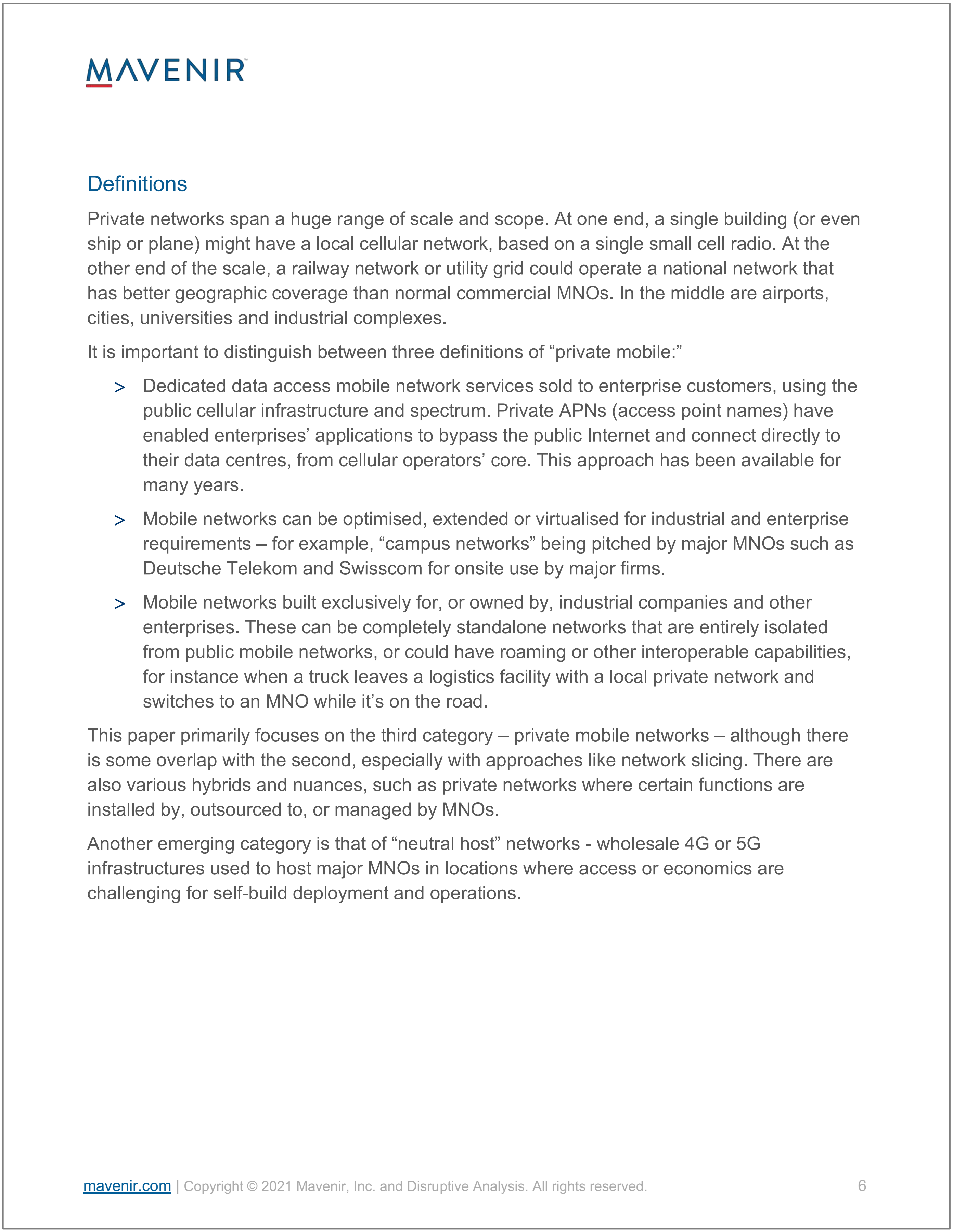
> Control: businesses often want a greater level of visibility and accountability for their networks, especially where they are used for business- or mission-critical applications. They prefer their own security and data/subscriber-management policies, and optimisations/upgrade cycles tuned for their own needs.

Commercials: in some cases, private LTE/5G networks are used to offer revenue-generating services for other third parties. Landlords may want to offer mobile connections to tenants (individuals or companies).

Numerous reasons for enterprises wanting to adopt private cellular

Coverage	Control	Cost	Compensation
• In-Building • Rural • Industrial • Offices • Road / Rail • Utility • Metro areas • Military / Govt	• Security • Sovereignty • Customised • Beyond Wi-Fi • Deployment • Lifecycle • Mobility • Private QoS	• Replace legacy LMR • Factory 4.0 • Replace Fiber • Avoid carrier per-GB fees • Own IoT connectivity	• Productivity • Private SIMs • Roaming • Local MVNO • Govt funding • Local FWA • MNO offload

Source: Disruptive Analysis



Definitions

Private networks span a huge range of scale and scope. At one end, a single building (or even ship or plane) might have a local cellular network, based on a single small cell radio. At the other end of the scale, a railway network or utility grid could operate a national network that has better geographic coverage than normal commercial MNOs. In the middle are airports, cities, universities and industrial complexes.

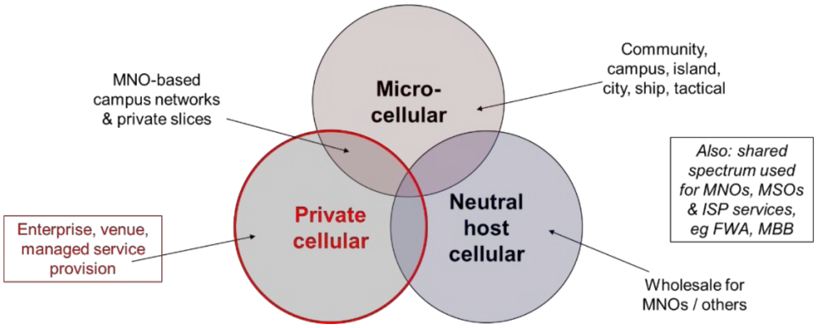
It is important to distinguish between three definitions of “private mobile:”

- Dedicated data access mobile network services sold to enterprise customers, using the public cellular infrastructure and spectrum. Private APNs (access point names) have enabled enterprises’ applications to bypass the public Internet and connect directly to their data centres, from cellular operators’ core. This approach has been available for many years.
- Mobile networks can be optimised, extended or virtualised for industrial and enterprise requirements – for example, “campus networks” being pitched by major MNOs such as Deutsche Telekom and Swisscom for onsite use by major firms.
- Mobile networks built exclusively for, or owned by, industrial companies and other enterprises. These can be completely standalone networks that are entirely isolated from public mobile networks, or could have roaming or other interoperable capabilities, for instance when a truck leaves a logistics facility with a local private network and switches to an MNO while it’s on the road.

This paper primarily focuses on the third category – private mobile networks – although there is some overlap with the second, especially with approaches like network slicing. There are also various hybrids and nuances, such as private networks where certain functions are installed by, outsourced to, or managed by MNOs.

Another emerging category is that of “neutral host” networks - wholesale 4G or 5G infrastructures used to host major MNOs in locations where access or economics are challenging for self-build deployment and operations.

Various overlapping categories of “non-public” mobile network are emerging



Source: Disruptive Analysis

Technical & regulatory enablers

There are demand and supply drivers for private cellular. Use cases and demand factors are considered in a separate section; here we look at the key technological evolutions and regulatory developments that are acting as catalysts for this new marketplace:

- Democratisation of 4G / 5G suitable spectrum
- Other forms of regulatory & policymaker support
- Virtualisation & cloudification of key control elements such as EPCs/5G Core, Edge Compute, eSIM and OSS/BSS
- Device & chipset support
- Small cells & Cloud/Open RAN
- Ecosystem readiness and maturity

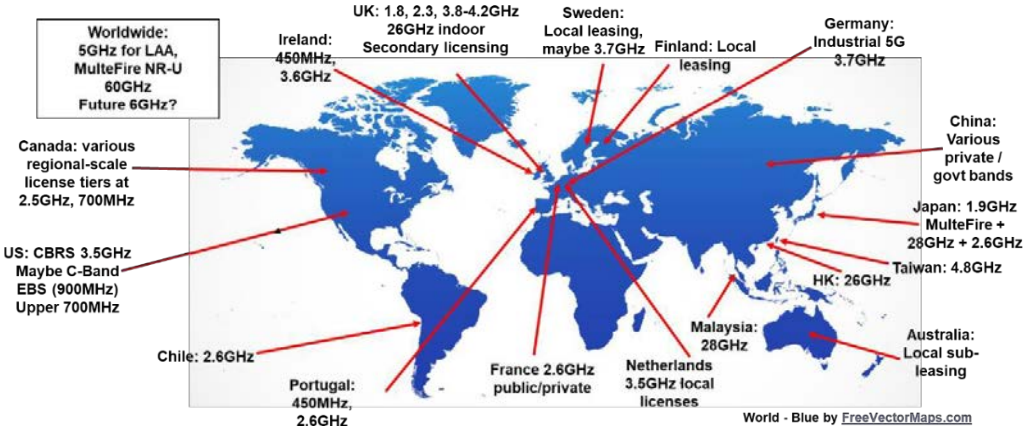
Democratising spectrum

Many conventional MNOs are working on “semi-private” networks for enterprise – typically campus networks which run in their normal spectrum bands, but which delegate some form of local autonomous control to an enterprise, via a private core network or virtual “slice” which is logically isolated from the main macro domain.

But what is far more disruptive is the advent of localised or shared spectrum allocations, which permit “non-public” networks to be built by enterprises themselves, or new classes of service provider and integrator. These can be standalone islands or can support roaming or sharing with the wider mobile universe.

Historically, local spectrum licenses have been available for point-to-point fixed links, temporary outside broadcast and events, private mobile radio and other purposes – but not in bands suitable for cellular networks.

Many countries are allocating spectrum suitable for private LTE / 5G networks



Source: Disruptive Analysis

Numerous countries have started to create flexible schemes suitable for private networks – although there is a large variability between national markets at present, in terms of rules, costs and license area sizes. Some interesting approaches include:

> **Dedicated licenses for specific sites.** For instance, Germany is releasing 3.7-3.8GHz frequencies for private 5G networks at industrial sites on a “first come, first served” basis. Swedish and Danish authorities are looking at something similar.

- > **MNOs leasing spectrum** in specific areas to enterprises or specialist providers. This occurs in markets such as Finland and Australia, to cover ports, mining, etc.
- > **"Dynamic access" spectrum sharing,** with database-driven systems and sensor networks for temporary or opportunistic allocation of spectrum. The US CBRS model is an example of this approach.
- > **Secondary re-use of national bands,** where they are not being actively used by the main licensee. The UK has recently adopted this model. It is similar to earlier TV "white space" models that aim to increase the efficiency of spectrum usage.
- > **Indoor-only permissions** for bands that avoid long-range interference with incumbent users because the signals do not pass through walls easily. The UK is looking at this model for 26GHz.
- > National licensing of spectrum for specific networks, such as for utility company grid control and IoT. This approach is seeing traction in markets such as Portugal and Ireland.

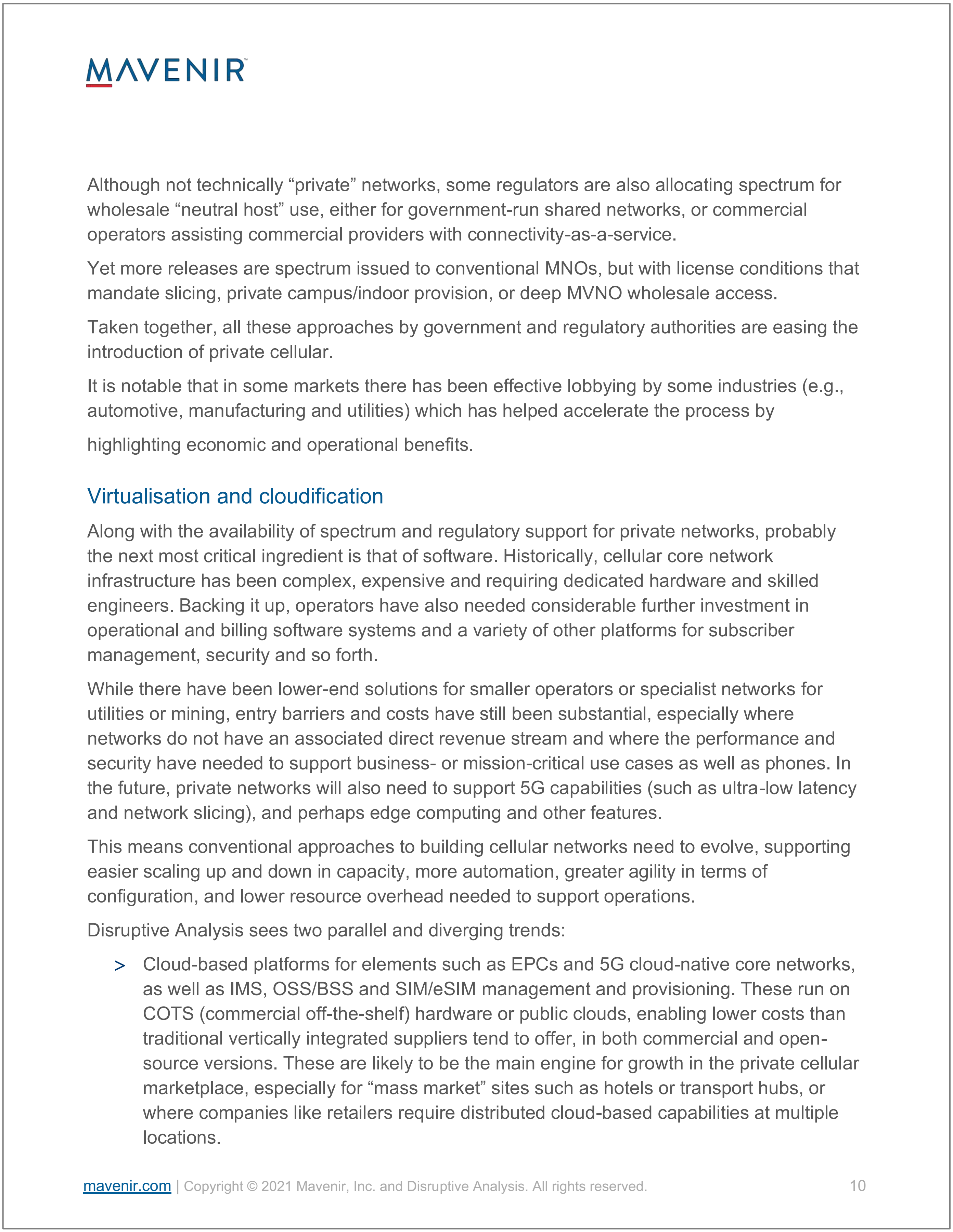
Disruptive Analysis expects the 2020-2022 period to show which models work best, with a second phase of spectrum releases – perhaps from 2024-2026 - incorporating lessons and best-practices. This will also parallel growing sophistication and maturity in spectrum databases, as well as more dynamic marketplaces for spectrum trading and rental.

Other forms of regulatory and government support

In addition to new spectrum models suitable for private LTE / 5G, various other shifts in the policy and regulatory world are making enterprise and vertical networks more viable.

These include:

- > Recognition of private networks' role in national broadband, 5G and industrial policy
- > "Barrier busting" task forces, which look at practical obstacles such as rights-of-way and cell tower / small cell siting regulations and processes
- > Government-funded testbeds and trials for 5G use cases and concepts
- > Government-owned cellular networks for public safety, transport, and metropolitan authorities
- > Other areas of telecoms regulation such as numbering, interconnect rules, applicability of lawful intercept rules and so forth



Although not technically “private” networks, some regulators are also allocating spectrum for wholesale “neutral host” use, either for government-run shared networks, or commercial operators assisting commercial providers with connectivity-as-a-service.

Yet more releases are spectrum issued to conventional MNOs, but with license conditions that mandate slicing, private campus/indoor provision, or deep MVNO wholesale access.

Taken together, all these approaches by government and regulatory authorities are easing the introduction of private cellular.

It is notable that in some markets there has been effective lobbying by some industries (e.g., automotive, manufacturing and utilities) which has helped accelerate the process by

highlighting economic and operational benefits.

Virtualisation and cloudification

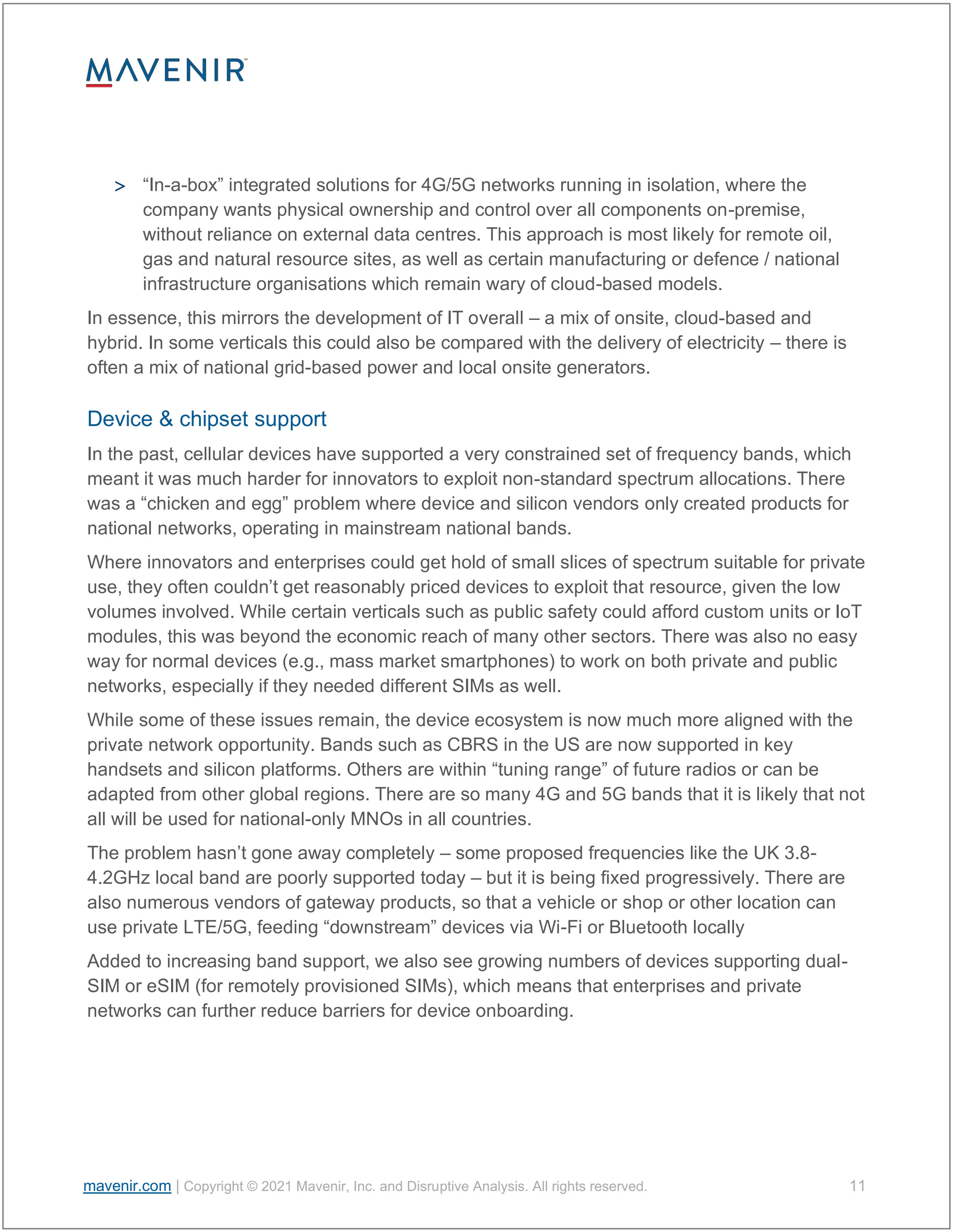
Along with the availability of spectrum and regulatory support for private networks, probably the next most critical ingredient is that of software. Historically, cellular core network infrastructure has been complex, expensive and requiring dedicated hardware and skilled engineers. Backing it up, operators have also needed considerable further investment in operational and billing software systems and a variety of other platforms for subscriber management, security and so forth.

While there have been lower-end solutions for smaller operators or specialist networks for utilities or mining, entry barriers and costs have still been substantial, especially where networks do not have an associated direct revenue stream and where the performance and security have needed to support business- or mission-critical use cases as well as phones. In the future, private networks will also need to support 5G capabilities (such as ultra-low latency and network slicing), and perhaps edge computing and other features.

This means conventional approaches to building cellular networks need to evolve, supporting easier scaling up and down in capacity, more automation, greater agility in terms of configuration, and lower resource overhead needed to support operations.

Disruptive Analysis sees two parallel and diverging trends:

- Cloud-based platforms for elements such as EPCs and 5G cloud-native core networks, as well as IMS, OSS/BSS and SIM/eSIM management and provisioning. These run on COTS (commercial off-the-shelf) hardware or public clouds, enabling lower costs than traditional vertically integrated suppliers tend to offer, in both commercial and open-source versions. These are likely to be the main engine for growth in the private cellular marketplace, especially for “mass market” sites such as hotels or transport hubs, or where companies like retailers require distributed cloud-based capabilities at multiple locations.



MAVENIR

- “In-a-box” integrated solutions for 4G/5G networks running in isolation, where the company wants physical ownership and control over all components on-premise, without reliance on external data centres. This approach is most likely for remote oil, gas and natural resource sites, as well as certain manufacturing or defence / national infrastructure organisations which remain wary of cloud-based models.

In essence, this mirrors the development of IT overall – a mix of onsite, cloud-based and hybrid. In some verticals this could also be compared with the delivery of electricity – there is often a mix of national grid-based power and local onsite generators.

Device & chipset support

In the past, cellular devices have supported a very constrained set of frequency bands, which meant it was much harder for innovators to exploit non-standard spectrum allocations. There was a “chicken and egg” problem where device and silicon vendors only created products for national networks, operating in mainstream national bands.

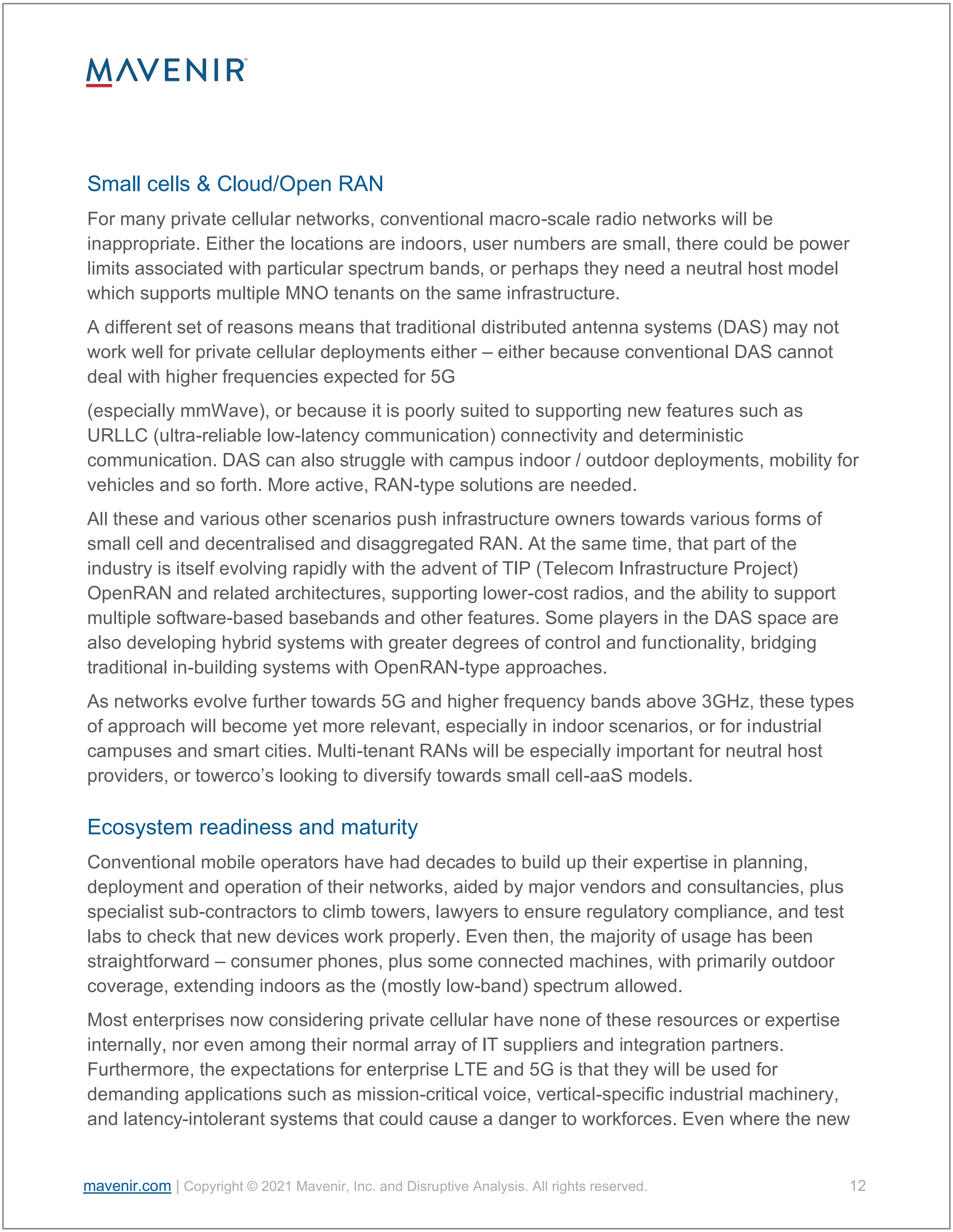
Where innovators and enterprises could get hold of small slices of spectrum suitable for private use, they often couldn’t get reasonably priced devices to exploit that resource, given the low volumes involved. While certain verticals such as public safety could afford custom units or IoT modules, this was beyond the economic reach of many other sectors. There was also no easy way for normal devices (e.g., mass market smartphones) to work on both private and public networks, especially if they needed different SIMs as well.

While some of these issues remain, the device ecosystem is now much more aligned with the private network opportunity. Bands such as CBRS in the US are now supported in key handsets and silicon platforms. Others are within “tuning range” of future radios or can be adapted from other global regions. There are so many 4G and 5G bands that it is likely that not all will be used for national-only MNOs in all countries.

The problem hasn’t gone away completely – some proposed frequencies like the UK 3.8-4.2GHz local band are poorly supported today – but it is being fixed progressively. There are also numerous vendors of gateway products, so that a vehicle or shop or other location can use private LTE/5G, feeding “downstream” devices via Wi-Fi or Bluetooth locally

Added to increasing band support, we also see growing numbers of devices supporting dual-SIM or eSIM (for remotely provisioned SIMs), which means that enterprises and private networks can further reduce barriers for device onboarding.

mavenir.com | Copyright © 2021 Mavenir, Inc. and Disruptive Analysis. All rights reserved. 11



Small cells & Cloud/Open RAN

For many private cellular networks, conventional macro-scale radio networks will be inappropriate. Either the locations are indoors, user numbers are small, there could be power limits associated with particular spectrum bands, or perhaps they need a neutral host model which supports multiple MNO tenants on the same infrastructure.

A different set of reasons means that traditional distributed antenna systems (DAS) may not work well for private cellular deployments either – either because conventional DAS cannot deal with higher frequencies expected for 5G

(especially mmWave), or because it is poorly suited to supporting new features such as URLLC (ultra-reliable low-latency communication) connectivity and deterministic communication. DAS can also struggle with campus indoor / outdoor deployments, mobility for vehicles and so forth. More active, RAN-type solutions are needed.

All these and various other scenarios push infrastructure owners towards various forms of small cell and decentralised and disaggregated RAN. At the same time, that part of the industry is itself evolving rapidly with the advent of TIP (Telecom Infrastructure Project) OpenRAN and related architectures, supporting lower-cost radios, and the ability to support multiple software-based basebands and other features. Some players in the DAS space are also developing hybrid systems with greater degrees of control and functionality, bridging traditional in-building systems with OpenRAN-type approaches.

As networks evolve further towards 5G and higher frequency bands above 3GHz, these types of approach will become yet more relevant, especially in indoor scenarios, or for industrial campuses and smart cities. Multi-tenant RANs will be especially important for neutral host providers, or towerco's looking to diversify towards small cell-aaS models.

Ecosystem readiness and maturity

Conventional mobile operators have had decades to build up their expertise in planning, deployment and operation of their networks, aided by major vendors and consultancies, plus specialist sub-contractors to climb towers, lawyers to ensure regulatory compliance, and test labs to check that new devices work properly. Even then, the majority of usage has been straightforward – consumer phones, plus some connected machines, with primarily outdoor coverage, extending indoors as the (mostly low-band) spectrum allowed.

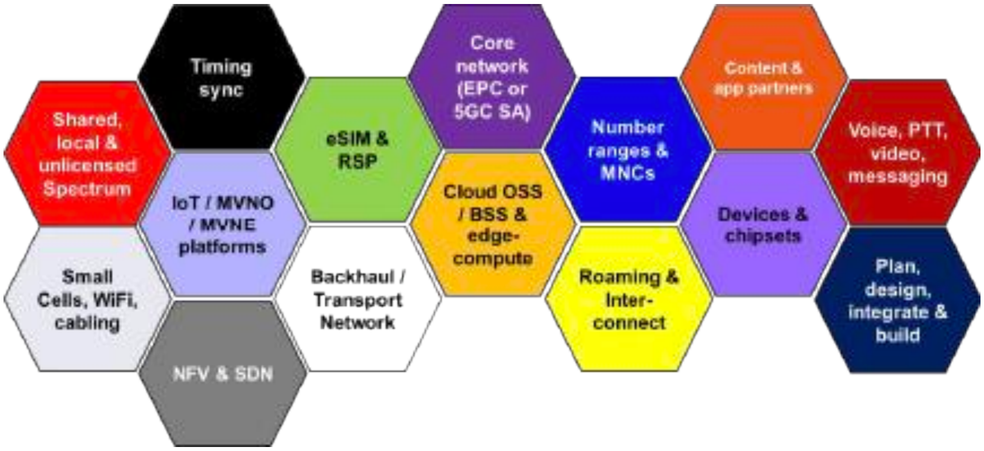
Most enterprises now considering private cellular have none of these resources or expertise internally, nor even among their normal array of IT suppliers and integration partners. Furthermore, the expectations for enterprise LTE and 5G is that they will be used for demanding applications such as mission-critical voice, vertical-specific industrial machinery, and latency-intolerant systems that could cause a danger to workforces. Even where the new networks are aimed at human guests or visitors, there will be difficulties around roaming, network sharing and commercial models.

For today’s existing private networks, a variety of specialist integrators and niche service providers have emerged, mostly fuelled by a cottage industry of vendors of small cells and core network components. Some of larger mobile equipment players have developed “special projects” units, while existing providers of critical communications gear (such as TETRA mobile radios) have added 4G systems to their portfolios.

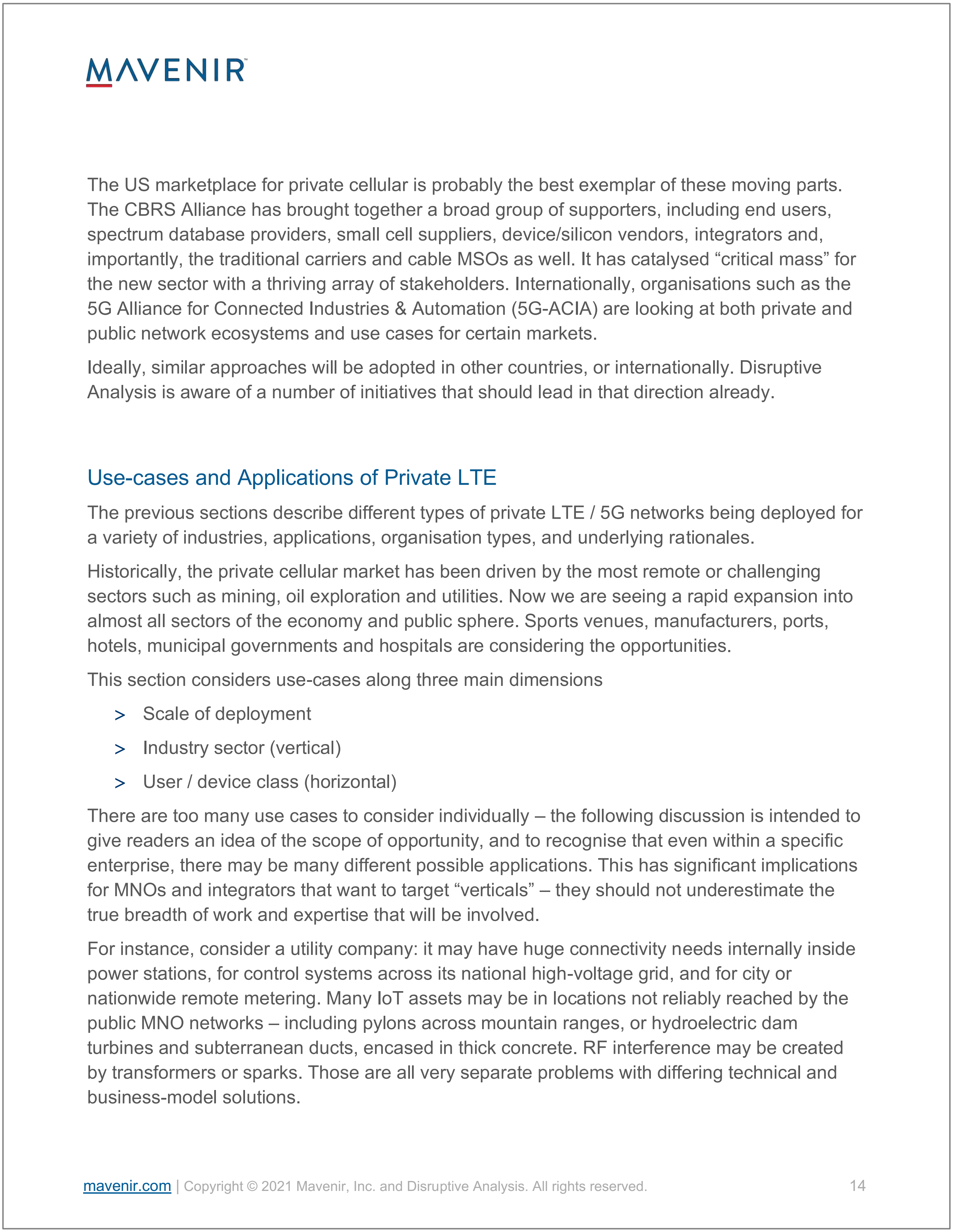
But this heavily customised “artisanal” approach is not scalable. The promise of truly “democratised” cellular, based on new spectrum releases and cloud-based platforms, will need more efficient channels and facilitators. The private LTE (and then 5G) sector will need to look more like the Wi-Fi industry, with “industrialised” deployment methods and multiple tiers of integrators and installers, especially for simpler and more straightforward implementations. Larger IT or industrial transformation projects will need to be able to incorporate cellular connectivity into their wider designs in routine fashion.

The real success of the new market will be heavily dependent on mature, accessible and diverse ecosystems. Ideally, industry organisations will bring together stakeholders, facilitate networking and partnerships, create baseline processes and design templates, publish case studies and identify gaps. There is also a need for training and certification.

Typical Maximum Power Consumption of a Single 5G Base Station


Shared, local & unlicensed Spectrum
Timing sync
IoT / MVNO / MVNE platforms
Small Cells, WiFi, cabling
NFV & SDN
eSIM & RSP
Backhaul / Transport Network
Core network (EPC or 5GC SA)
Cloud OSS / BSS & edge-compute
Number ranges & MNCs
Roaming & Inter-connect
Content & app partners
Devices & chipsets
Voice, PTT, video, messaging
Plan, design, integrate & build

Source: Disruptive Analysis



The US marketplace for private cellular is probably the best exemplar of these moving parts. The CBRS Alliance has brought together a broad group of supporters, including end users, spectrum database providers, small cell suppliers, device/silicon vendors, integrators and, importantly, the traditional carriers and cable MSOs as well. It has catalysed “critical mass” for the new sector with a thriving array of stakeholders. Internationally, organisations such as the 5G Alliance for Connected Industries & Automation (5G-ACIA) are looking at both private and public network ecosystems and use cases for certain markets.

Ideally, similar approaches will be adopted in other countries, or internationally. Disruptive Analysis is aware of a number of initiatives that should lead in that direction already.

Use-cases and Applications of Private LTE

The previous sections describe different types of private LTE / 5G networks being deployed for a variety of industries, applications, organisation types, and underlying rationales.

Historically, the private cellular market has been driven by the most remote or challenging sectors such as mining, oil exploration and utilities. Now we are seeing a rapid expansion into almost all sectors of the economy and public sphere. Sports venues, manufacturers, ports, hotels, municipal governments and hospitals are considering the opportunities.

This section considers use-cases along three main dimensions

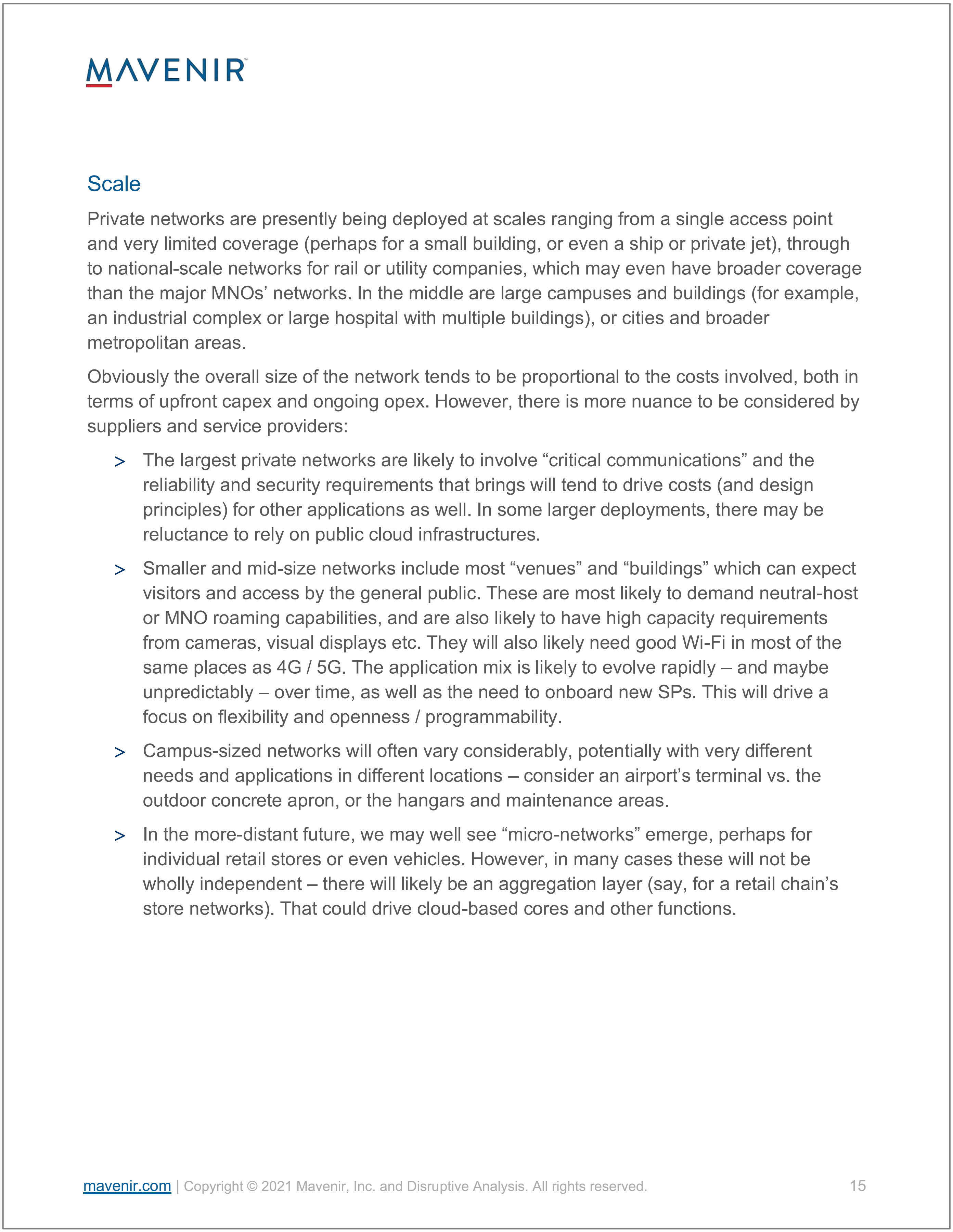
> Scale of deployment

> Industry sector (vertical)

> User / device class (horizontal)

There are too many use cases to consider individually – the following discussion is intended to give readers an idea of the scope of opportunity, and to recognise that even within a specific enterprise, there may be many different possible applications. This has significant implications for MNOs and integrators that want to target “verticals” – they should not underestimate the true breadth of work and expertise that will be involved.

For instance, consider a utility company: it may have huge connectivity needs internally inside power stations, for control systems across its national high-voltage grid, and for city or nationwide remote metering. Many IoT assets may be in locations not reliably reached by the public MNO networks – including pylons across mountain ranges, or hydroelectric dam turbines and subterranean ducts, encased in thick concrete. RF interference may be created by transformers or sparks. Those are all very separate problems with differing technical and business-model solutions.



Scale

Private networks are presently being deployed at scales ranging from a single access point and very limited coverage (perhaps for a small building, or even a ship or private jet), through to national-scale networks for rail or utility companies, which may even have broader coverage than the major MNOs' networks. In the middle are large campuses and buildings (for example, an industrial complex or large hospital with multiple buildings), or cities and broader metropolitan areas.

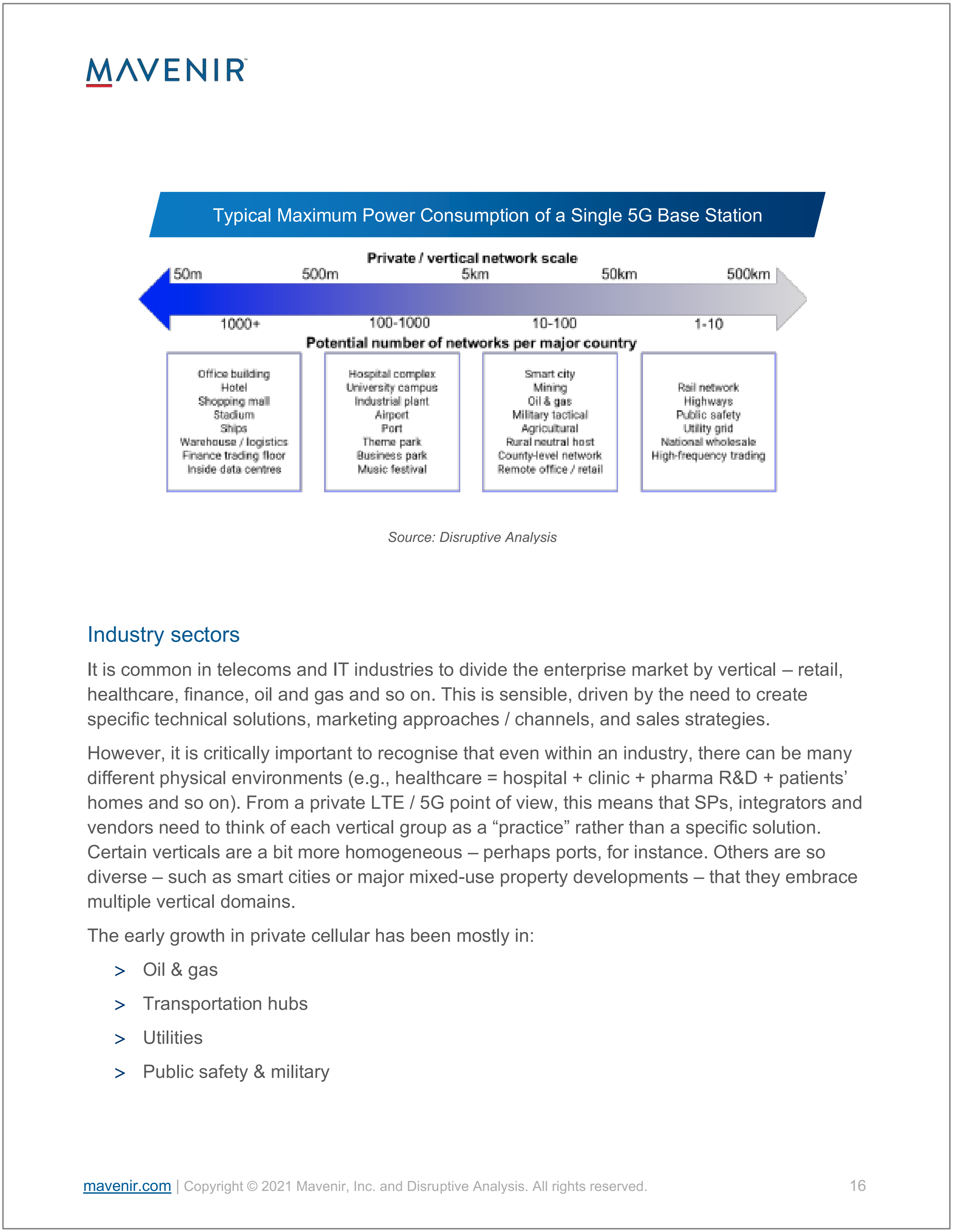
Obviously the overall size of the network tends to be proportional to the costs involved, both in terms of upfront capex and ongoing opex. However, there is more nuance to be considered by suppliers and service providers:

> The largest private networks are likely to involve "critical communications" and the reliability and security requirements that brings will tend to drive costs (and design principles) for other applications as well. In some larger deployments, there may be reluctance to rely on public cloud infrastructures.

> Smaller and mid-size networks include most "venues" and "buildings" which can expect visitors and access by the general public. These are most likely to demand neutral-host or MNO roaming capabilities, and are also likely to have high capacity requirements from cameras, visual displays etc. They will also likely need good Wi-Fi in most of the same places as 4G / 5G. The application mix is likely to evolve rapidly – and maybe unpredictably – over time, as well as the need to onboard new SPs. This will drive a focus on flexibility and openness / programmability.

> Campus-sized networks will often vary considerably, potentially with very different needs and applications in different locations – consider an airport's terminal vs. the outdoor concrete apron, or the hangars and maintenance areas.

> In the more-distant future, we may well see "micro-networks" emerge, perhaps for individual retail stores or even vehicles. However, in many cases these will not be wholly independent – there will likely be an aggregation layer (say, for a retail chain's store networks). That could drive cloud-based cores and other functions.



MAVENIR

Typical Maximum Power Consumption of a Single 5G Base Station

Private / vertical network scale

50m 500m 5km 50km 500km

1000+ 100-1000 10-100 1-10

Potential number of networks per major country

1000+	100-1000	10-100	1-10
Office building Hotel Shopping mall Stadium Ships Warehouse / logistics Finance trading floor Inside data centres	Hospital complex University campus Industrial plant Airport Port Theme park Business park Music festival	Smart city Mining Oil & gas Military tactical Agricultural Rural neutral host County-level network Remote office / retail	Rail network Highways Public safety Utility grid National wholesale High-frequency trading

Source: Disruptive Analysis

Industry sectors

It is common in telecoms and IT industries to divide the enterprise market by vertical – retail, healthcare, finance, oil and gas and so on. This is sensible, driven by the need to create specific technical solutions, marketing approaches / channels, and sales strategies.

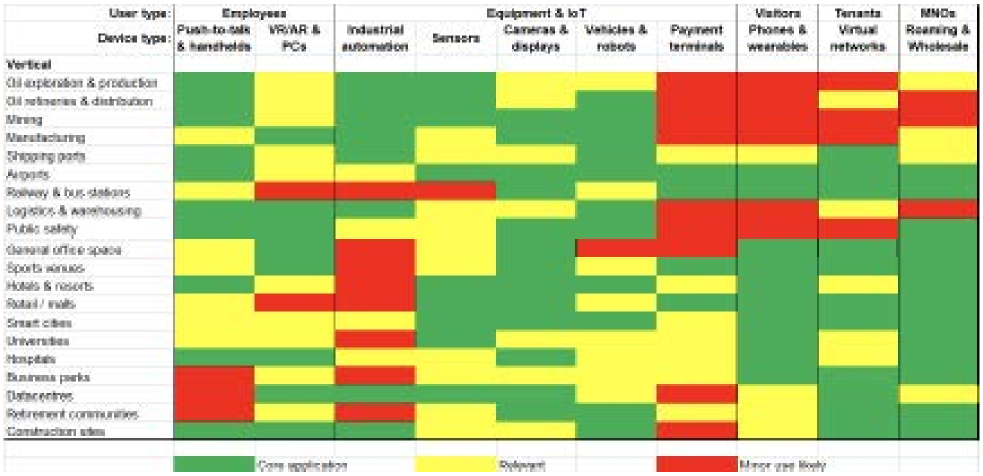
However, it is critically important to recognise that even within an industry, there can be many different physical environments (e.g., healthcare = hospital + clinic + pharma R&D + patients' homes and so on). From a private LTE / 5G point of view, this means that SPs, integrators and vendors need to think of each vertical group as a "practice" rather than a specific solution. Certain verticals are a bit more homogeneous – perhaps ports, for instance. Others are so diverse – such as smart cities or major mixed-use property developments – that they embrace multiple vertical domains.

The early growth in private cellular has been mostly in:

- Oil & gas
- Transportation hubs
- Utilities
- Public safety & military

That has been driven by spectrum availability and because these have often been cost-insensitive. Many are unable to use Wi-Fi or fixed connections for many of their applications, especially vehicular or push-to-talk.

Typical Maximum Power Consumption of a Single 5G Base Station



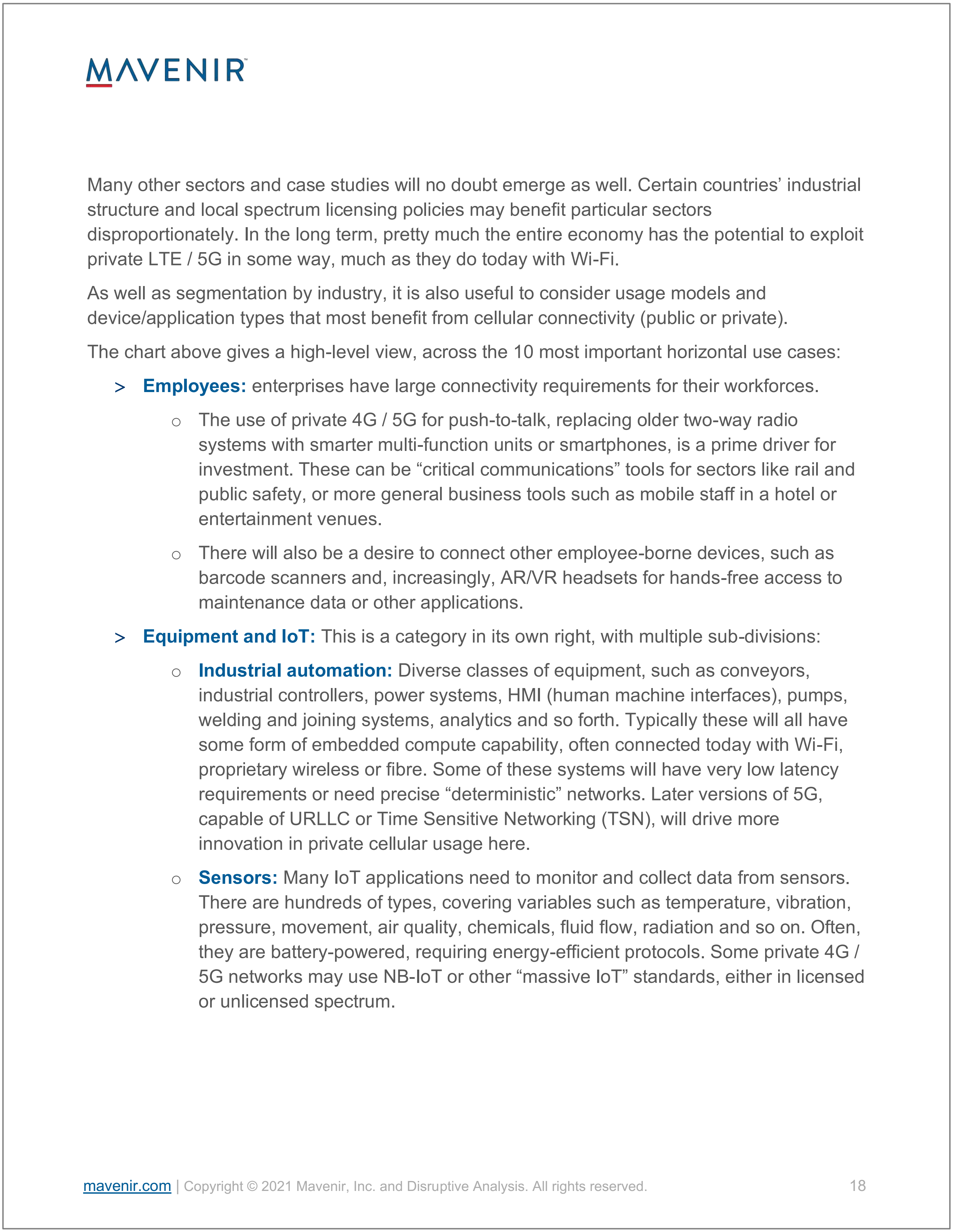
User type:	Employees		Equipment & IoT					Visitors	Tenants	MNOs
Device type:	Push-to-talk & handhelds	VR/AR & PCs	Industrial automation	Sensors	Cameras & displays	Vehicles & robots	Payment terminals	Phones & wearables	Virtual networks	Roaming & Wholesale
Vertical										
Oil exploration & production	🟩	🟨	🟩	🟩	🟨	🟨	🟥	🟥	🟥	🟨
Oil refineries & distribution	🟩	🟨	🟩	🟩	🟨	🟩	🟥	🟥	🟨	🟥
Mining	🟩	🟨	🟩	🟩	🟩	🟩	🟥	🟥	🟥	🟥
Manufacturing	🟨	🟩	🟩	🟨	🟩	🟩	🟥	🟥	🟥	🟨
Shipping ports	🟩	🟨	🟩	🟨	🟨	🟩	🟨	🟨	🟩	🟨
Airports	🟩	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Railway & bus stations	🟨	🟥	🟥	🟥	🟩	🟨	🟩	🟩	🟩	🟩
Logistics & warehousing	🟩	🟩	🟩	🟨	🟨	🟩	🟥	🟥	🟨	🟥
Public safety	🟩	🟩	🟨	🟨	🟩	🟩	🟥	🟥	🟥	🟩
General office space	🟨	🟩	🟥	🟨	🟩	🟥	🟥	🟩	🟩	🟩
Sports venues	🟨	🟩	🟥	🟨	🟩	🟨	🟩	🟩	🟩	🟩
Hotels & resorts	🟩	🟨	🟥	🟩	🟩	🟩	🟨	🟩	🟨	🟩
Retail / malls	🟨	🟥	🟥	🟩	🟩	🟨	🟩	🟩	🟩	🟩
Smart cities	🟨	🟨	🟨	🟩	🟩	🟩	🟨	🟩	🟩	🟩
Universities	🟨	🟨	🟥	🟩	🟨	🟨	🟨	🟩	🟨	🟩
Hospitals	🟩	🟩	🟨	🟨	🟩	🟨	🟨	🟩	🟨	🟩
Business parks	🟥	🟨	🟥	🟨	🟨	🟨	🟨	🟩	🟩	🟩
Datacentres	🟥	🟩	🟩	🟩	🟩	🟨	🟥	🟨	🟩	🟨
Retirement communities	🟥	🟨	🟥	🟨	🟩	🟩	🟨	🟨	🟩	🟩
Construction sites	🟩	🟩	🟩	🟨	🟨	🟩	🟥	🟨	🟩	🟩

🟩 Core application 🟨 Relevant 🟥 Minor use likely

Source: Disruptive Analysis

Over the next 5 years, readers should expect much stronger growth in private LTE/5G in:

- Manufacturing (although with long design / prototype cycles)
- Logistics and warehousing (very IoT-centric e.g., robots in fulfilment centres)
- Sports and entertainment venues (initially for “back office” users like broadcasters)
- Smart cities & business parks (with a lot of diversity in early usage & applications)
- Airports (especially “airside” rather than “landside”)
- Hotels & resorts (initially staff, then moving to guests and neutral host over time)



Many other sectors and case studies will no doubt emerge as well. Certain countries' industrial structure and local spectrum licensing policies may benefit particular sectors disproportionately. In the long term, pretty much the entire economy has the potential to exploit private LTE / 5G in some way, much as they do today with Wi-Fi.

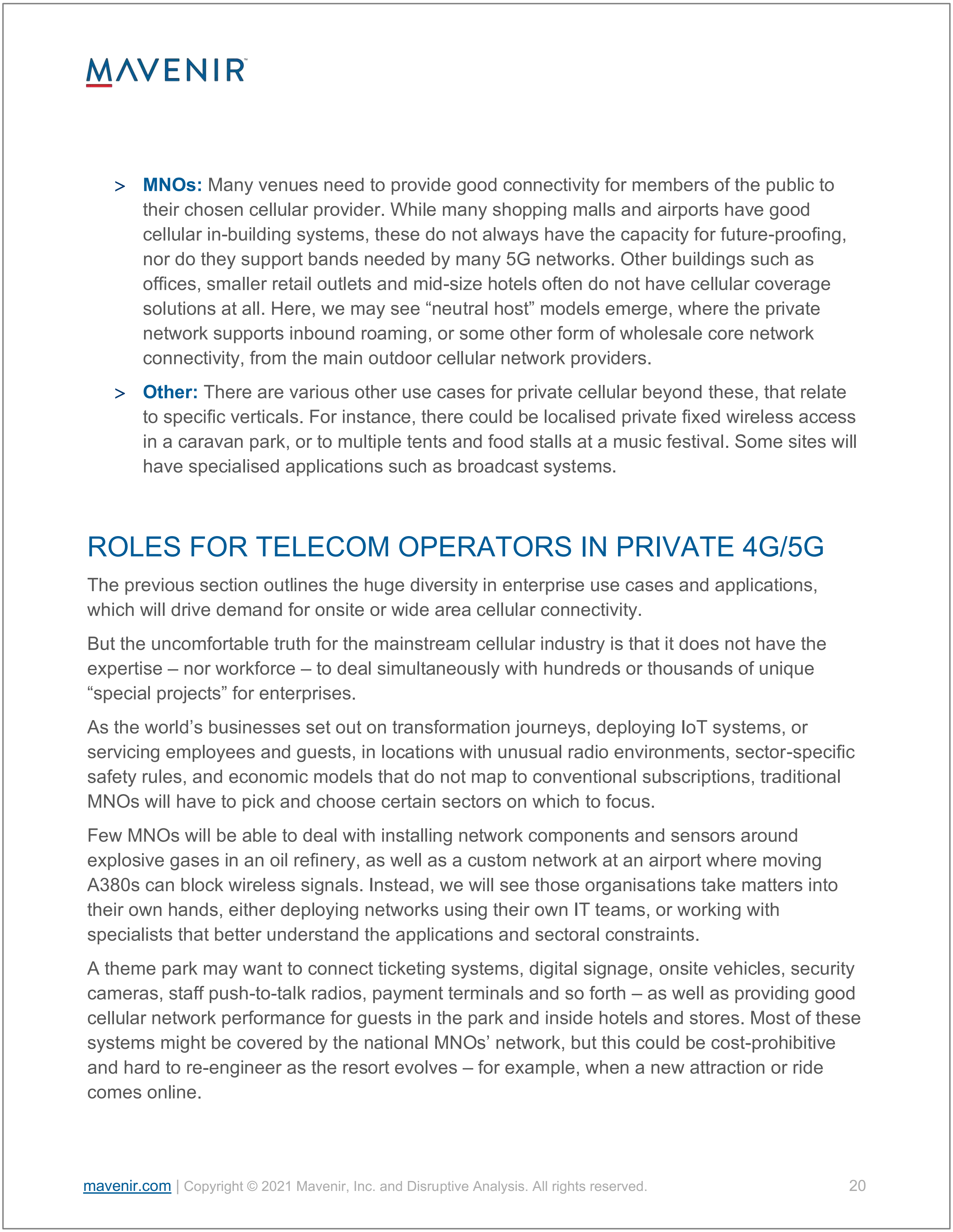
As well as segmentation by industry, it is also useful to consider usage models and device/application types that most benefit from cellular connectivity (public or private).

The chart above gives a high-level view, across the 10 most important horizontal use cases:

- **Employees:** enterprises have large connectivity requirements for their workforces.
  - The use of private 4G / 5G for push-to-talk, replacing older two-way radio systems with smarter multi-function units or smartphones, is a prime driver for investment. These can be "critical communications" tools for sectors like rail and public safety, or more general business tools such as mobile staff in a hotel or entertainment venues.
  - There will also be a desire to connect other employee-borne devices, such as barcode scanners and, increasingly, AR/VR headsets for hands-free access to maintenance data or other applications.
- **Equipment and IoT:** This is a category in its own right, with multiple sub-divisions:
  - **Industrial automation:** Diverse classes of equipment, such as conveyors, industrial controllers, power systems, HMI (human machine interfaces), pumps, welding and joining systems, analytics and so forth. Typically these will all have some form of embedded compute capability, often connected today with Wi-Fi, proprietary wireless or fibre. Some of these systems will have very low latency requirements or need precise "deterministic" networks. Later versions of 5G, capable of URLLC or Time Sensitive Networking (TSN), will drive more innovation in private cellular usage here.
  - **Sensors:** Many IoT applications need to monitor and collect data from sensors. There are hundreds of types, covering variables such as temperature, vibration, pressure, movement, air quality, chemicals, fluid flow, radiation and so on. Often, they are battery-powered, requiring energy-efficient protocols. Some private 4G / 5G networks may use NB-IoT or other "massive IoT" standards, either in licensed or unlicensed spectrum.

  - **Cameras and displays:** A large % of wireless data is expected to be driven by images and video – either capturing / uploading from camera or display via the ever proliferating numbers of digital displays. There are many use cases here, from security cameras, to advertising boards, to real-time image analysis for quality control in manufacturing.
  - **Vehicles and robots:** Many industries employ moving systems on their campus sites or across wider areas. These will almost always need wireless connectivity for control, or perhaps remote-driving or onboard communications. This includes autonomous guided vehicles (AGVs) in factories or ports, tractors in agriculture, human-transportation pods in retirement villages, drones for aerial inspection on construction sites or chemical plants, and many others. These systems need careful network planning, prioritisation, latency and reliability, especially for safety reasons.
  - **Payment systems:** Many high footfall locations have transaction-based systems such as payment terminals, ticketing machines, ATMs and so on. Today, many use the same (congested) Wi-Fi that staff and visitors use for smartphones and other devices. They may be deep inside buildings, with little coverage from outdoor MNO networks. As they are often business-critical, there is a clear desire to offload the connections to localised, private-managed and uncongested cellular. There is also a strong security-based argument for putting these on an isolated network.

- **Visitors and guests:** In many locations, visitors expect continuous coverage from their normal MNO. But they may prefer to obtain new, local connectivity – for example to avoid international roaming fees. While Wi-Fi is prevalent, there is also a need for cellular connectivity, both for smartphones and other devices. Private LTE / 5G networks could also enable venue owners to offer “free 5G,” similar to Wi-Fi, perhaps monetising with advertising or social media connections. Contractors on enterprise sites (for instance auditors, or sub-contract construction engineers) could also use the local connectivity provided by the IT staff.
- **Tenants:** Some private 4G / 5G networks will operate like a small public MNO, where the tenants (individuals or separate businesses) are their “subscribers.” This includes residential multi-dwelling units (which already provide fixed broadband to apartments), or locations such as airports or shopping malls or shared office space, with onsite businesses wanting connectivity for their employees and other systems. This model already works – Heathrow Airport offers telecom services to caterers and maintenance companies, and Southern Linc (part of a US utility firm) offers managed push-to-talk for other critical-comms users in several US states.



- **MNOs:** Many venues need to provide good connectivity for members of the public to their chosen cellular provider. While many shopping malls and airports have good cellular in-building systems, these do not always have the capacity for future-proofing, nor do they support bands needed by many 5G networks. Other buildings such as offices, smaller retail outlets and mid-size hotels often do not have cellular coverage solutions at all. Here, we may see “neutral host” models emerge, where the private network supports inbound roaming, or some other form of wholesale core network connectivity, from the main outdoor cellular network providers.
- **Other:** There are various other use cases for private cellular beyond these, that relate to specific verticals. For instance, there could be localised private fixed wireless access in a caravan park, or to multiple tents and food stalls at a music festival. Some sites will have specialised applications such as broadcast systems.

ROLES FOR TELECOM OPERATORS IN PRIVATE 4G/5G

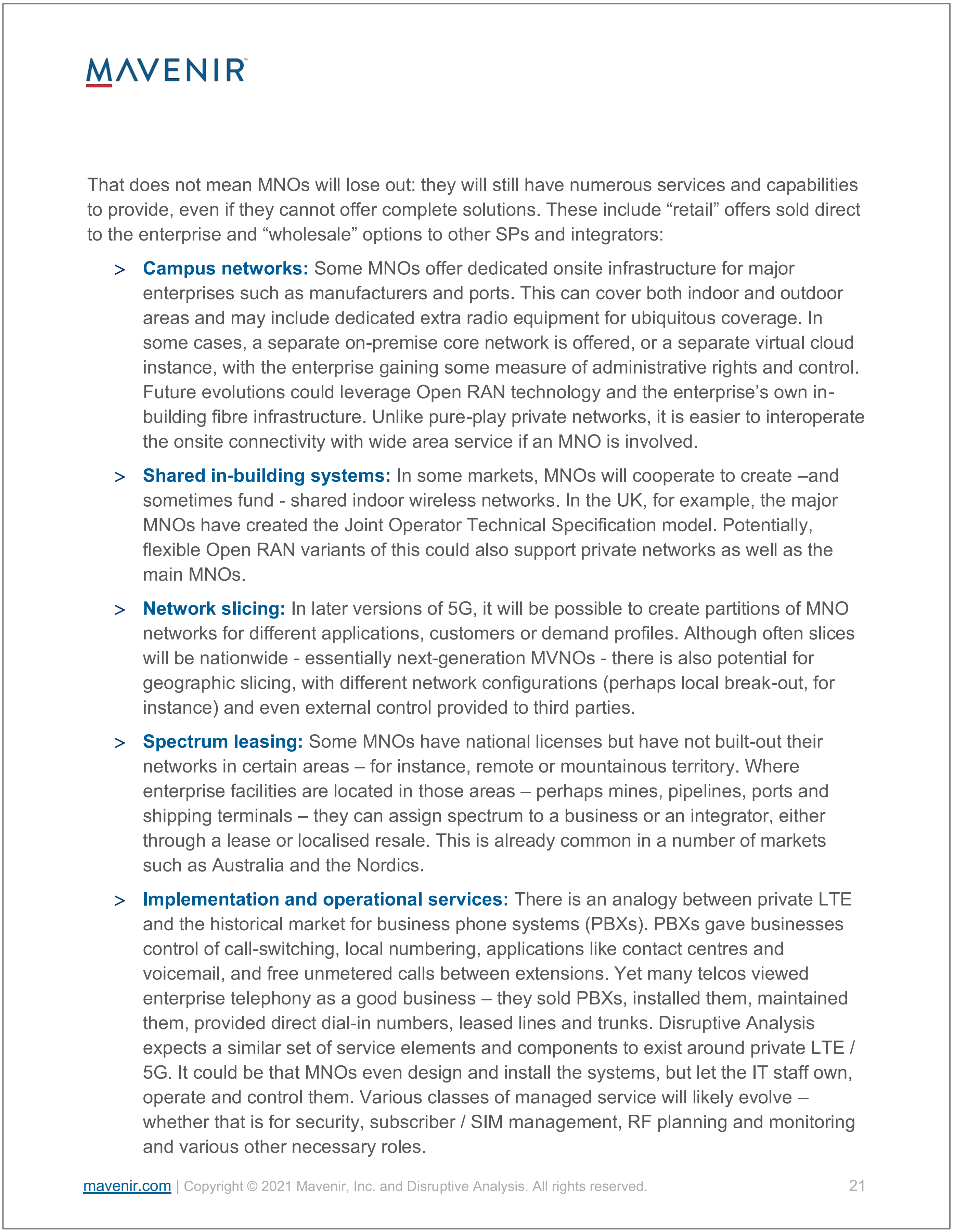
The previous section outlines the huge diversity in enterprise use cases and applications, which will drive demand for onsite or wide area cellular connectivity.

But the uncomfortable truth for the mainstream cellular industry is that it does not have the expertise – nor workforce – to deal simultaneously with hundreds or thousands of unique “special projects” for enterprises.

As the world’s businesses set out on transformation journeys, deploying IoT systems, or servicing employees and guests, in locations with unusual radio environments, sector-specific safety rules, and economic models that do not map to conventional subscriptions, traditional MNOs will have to pick and choose certain sectors on which to focus.

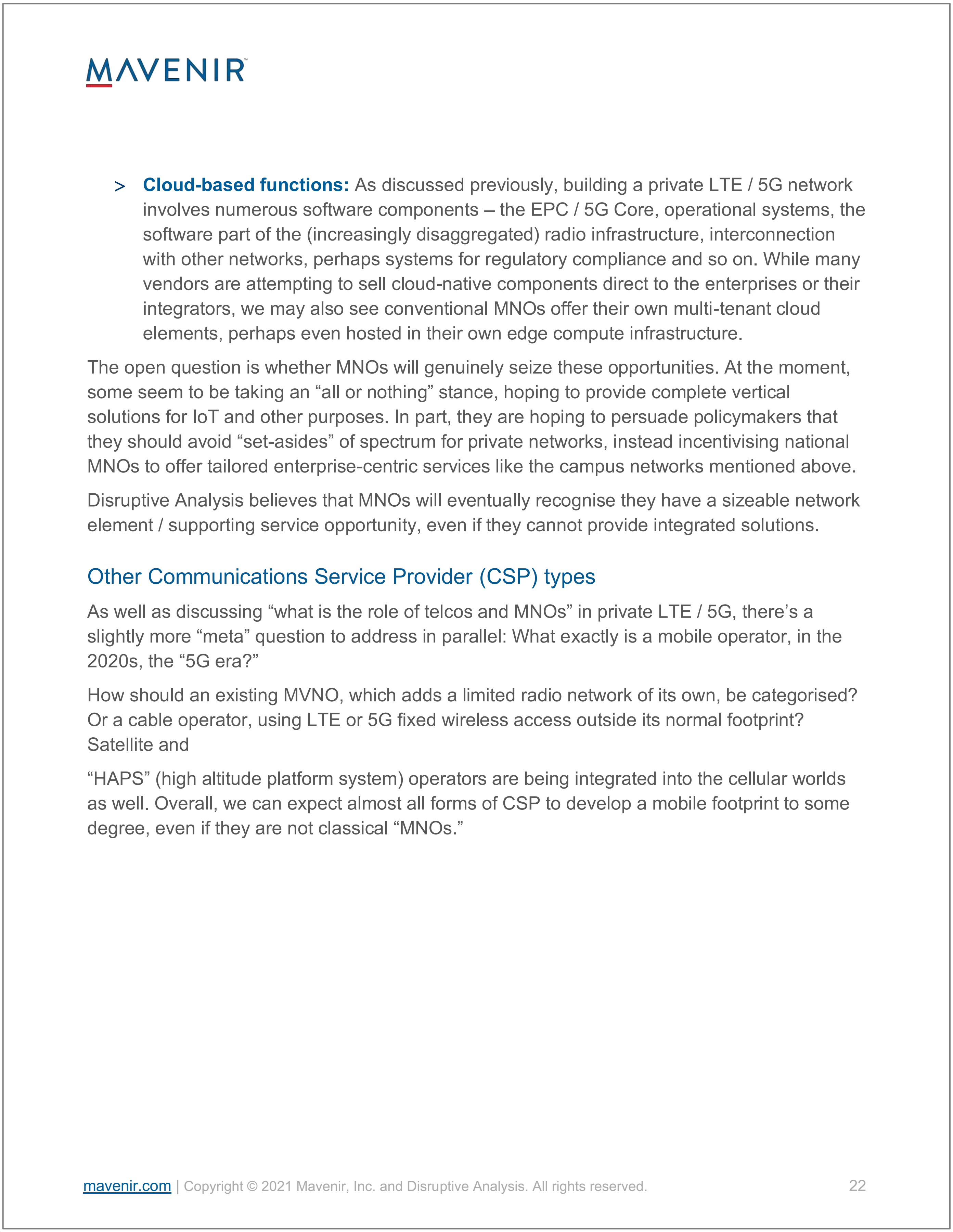
Few MNOs will be able to deal with installing network components and sensors around explosive gases in an oil refinery, as well as a custom network at an airport where moving A380s can block wireless signals. Instead, we will see those organisations take matters into their own hands, either deploying networks using their own IT teams, or working with specialists that better understand the applications and sectoral constraints.

A theme park may want to connect ticketing systems, digital signage, onsite vehicles, security cameras, staff push-to-talk radios, payment terminals and so forth – as well as providing good cellular network performance for guests in the park and inside hotels and stores. Most of these systems might be covered by the national MNOs’ network, but this could be cost-prohibitive and hard to re-engineer as the resort evolves – for example, when a new attraction or ride comes online.



That does not mean MNOs will lose out: they will still have numerous services and capabilities to provide, even if they cannot offer complete solutions. These include “retail” offers sold direct to the enterprise and “wholesale” options to other SPs and integrators:

- **Campus networks:** Some MNOs offer dedicated onsite infrastructure for major enterprises such as manufacturers and ports. This can cover both indoor and outdoor areas and may include dedicated extra radio equipment for ubiquitous coverage. In some cases, a separate on-premise core network is offered, or a separate virtual cloud instance, with the enterprise gaining some measure of administrative rights and control. Future evolutions could leverage Open RAN technology and the enterprise’s own in-building fibre infrastructure. Unlike pure-play private networks, it is easier to interoperate the onsite connectivity with wide area service if an MNO is involved.
- **Shared in-building systems:** In some markets, MNOs will cooperate to create –and sometimes fund - shared indoor wireless networks. In the UK, for example, the major MNOs have created the Joint Operator Technical Specification model. Potentially, flexible Open RAN variants of this could also support private networks as well as the main MNOs.
- **Network slicing:** In later versions of 5G, it will be possible to create partitions of MNO networks for different applications, customers or demand profiles. Although often slices will be nationwide - essentially next-generation MVNOs - there is also potential for geographic slicing, with different network configurations (perhaps local break-out, for instance) and even external control provided to third parties.
- **Spectrum leasing:** Some MNOs have national licenses but have not built-out their networks in certain areas – for instance, remote or mountainous territory. Where enterprise facilities are located in those areas – perhaps mines, pipelines, ports and shipping terminals – they can assign spectrum to a business or an integrator, either through a lease or localised resale. This is already common in a number of markets such as Australia and the Nordics.
- **Implementation and operational services:** There is an analogy between private LTE and the historical market for business phone systems (PBXs). PBXs gave businesses control of call-switching, local numbering, applications like contact centres and voicemail, and free unmetered calls between extensions. Yet many telcos viewed enterprise telephony as a good business – they sold PBXs, installed them, maintained them, provided direct dial-in numbers, leased lines and trunks. Disruptive Analysis expects a similar set of service elements and components to exist around private LTE / 5G. It could be that MNOs even design and install the systems, but let the IT staff own, operate and control them. Various classes of managed service will likely evolve – whether that is for security, subscriber / SIM management, RF planning and monitoring and various other necessary roles.



- **Cloud-based functions:** As discussed previously, building a private LTE / 5G network involves numerous software components – the EPC / 5G Core, operational systems, the software part of the (increasingly disaggregated) radio infrastructure, interconnection with other networks, perhaps systems for regulatory compliance and so on. While many vendors are attempting to sell cloud-native components direct to the enterprises or their integrators, we may also see conventional MNOs offer their own multi-tenant cloud elements, perhaps even hosted in their own edge compute infrastructure.

The open question is whether MNOs will genuinely seize these opportunities. At the moment, some seem to be taking an “all or nothing” stance, hoping to provide complete vertical solutions for IoT and other purposes. In part, they are hoping to persuade policymakers that they should avoid “set-asides” of spectrum for private networks, instead incentivising national MNOs to offer tailored enterprise-centric services like the campus networks mentioned above.

Disruptive Analysis believes that MNOs will eventually recognise they have a sizeable network element / supporting service opportunity, even if they cannot provide integrated solutions.

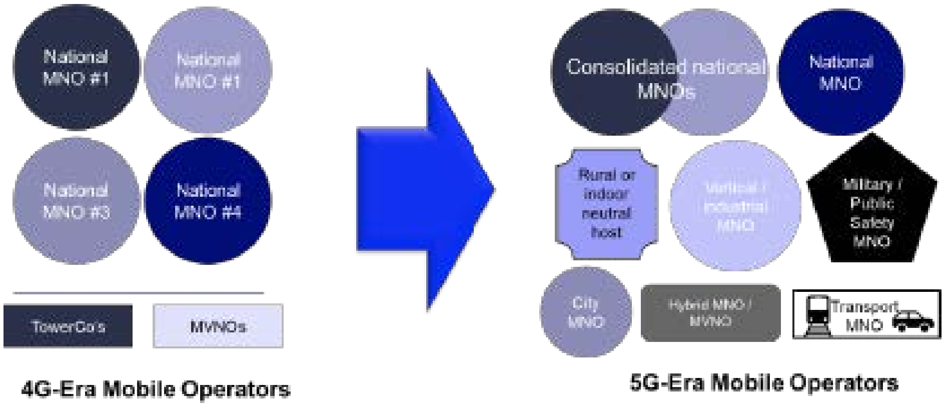
Other Communications Service Provider (CSP) types

As well as discussing “what is the role of telcos and MNOs” in private LTE / 5G, there’s a slightly more “meta” question to address in parallel: What exactly is a mobile operator, in the 2020s, the “5G era?”

How should an existing MVNO, which adds a limited radio network of its own, be categorised? Or a cable operator, using LTE or 5G fixed wireless access outside its normal footprint? Satellite and

“HAPS” (high altitude platform system) operators are being integrated into the cellular worlds as well. Overall, we can expect almost all forms of CSP to develop a mobile footprint to some degree, even if they are not classical “MNOs.”

Typical Maximum Power Consumption of a Single 5G Base Station

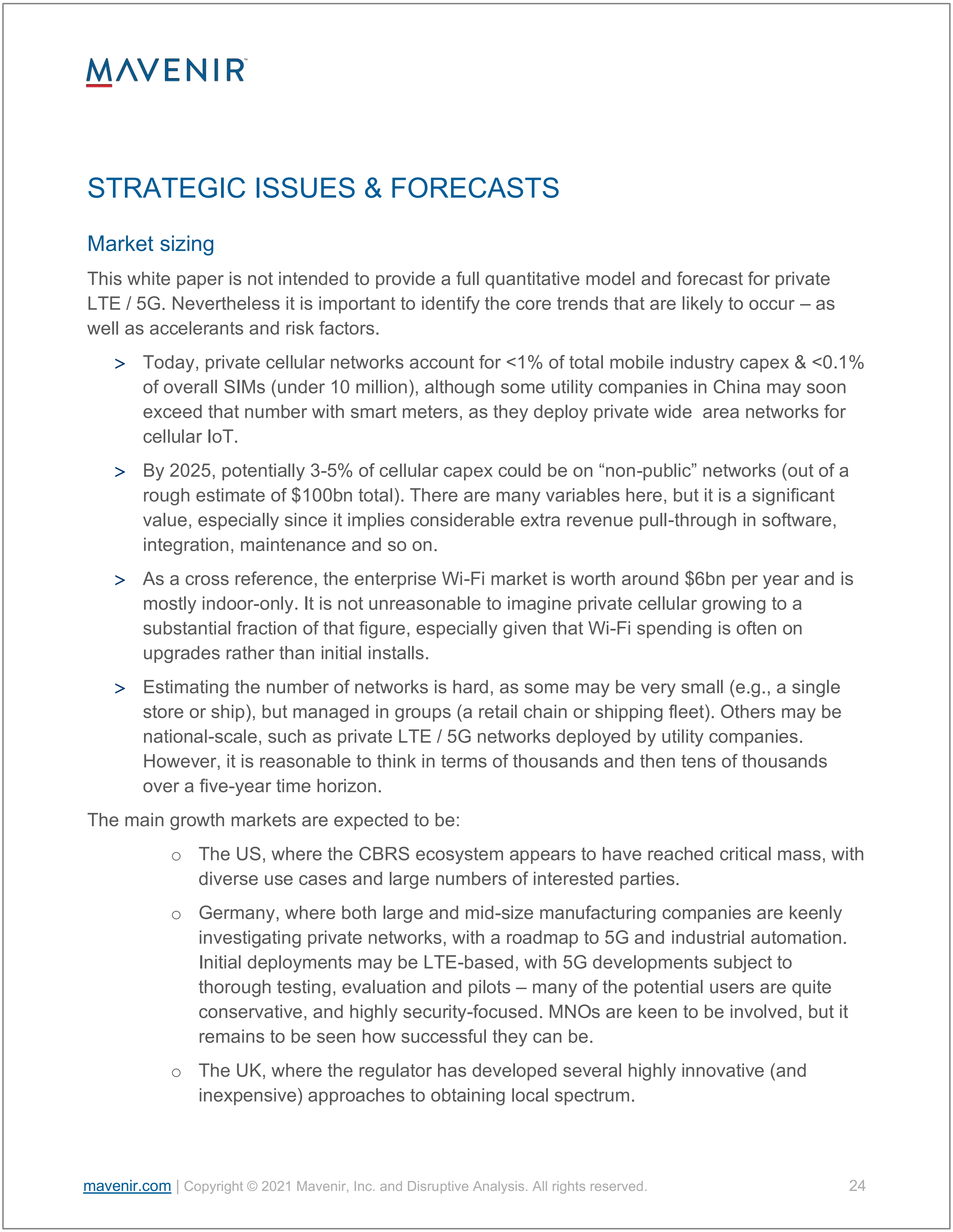


Source: Disruptive Analysis

While a single enterprise running its own internal network, solely for its employees and IoT devices, cannot really be described as a service provider, the definition gets much cloudier when you consider metro-scale MNOs (for instance, in Austria, where recent spectrum auctions created four new regional-scale operators or consortia).

We will also see the entry of various "new telcos" as well as IT and industrial solution integrators operating in new shared-spectrum bands, on behalf of their enterprise clients. Sometimes they will obtain frequencies directly through the various new release mechanisms, and in other cases they may lease or rent spectrum from incumbent MNOs.

Overall, Disruptive Analysis expects the distinction between "public" and "non-public" network to become far less clear. This will prompt re-evaluation by regulators, investors and enterprises themselves.



STRATEGIC ISSUES & FORECASTS

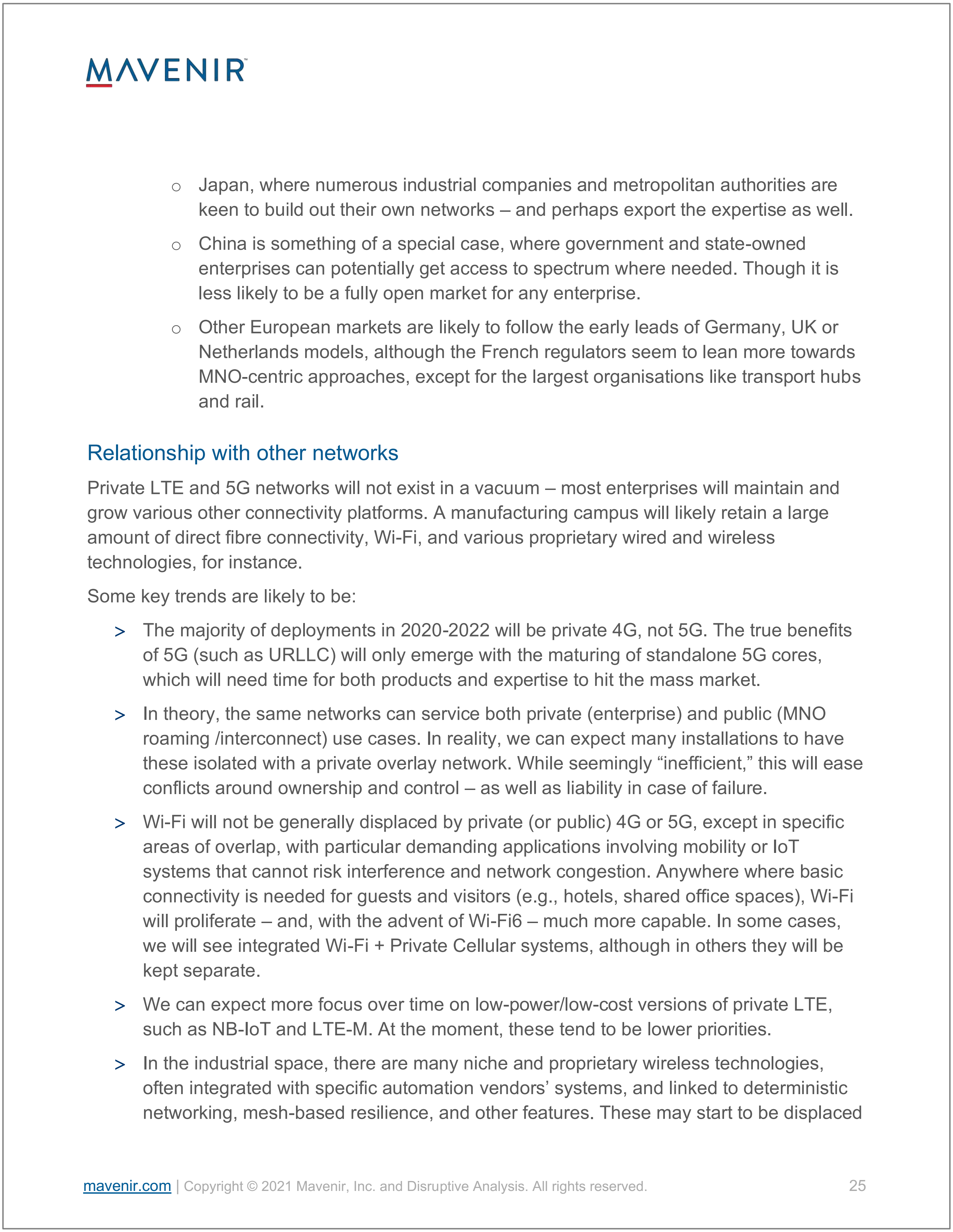
Market sizing

This white paper is not intended to provide a full quantitative model and forecast for private LTE / 5G. Nevertheless it is important to identify the core trends that are likely to occur – as well as accelerants and risk factors.

- Today, private cellular networks account for <1% of total mobile industry capex & <0.1% of overall SIMs (under 10 million), although some utility companies in China may soon exceed that number with smart meters, as they deploy private wide area networks for cellular IoT.
- By 2025, potentially 3-5% of cellular capex could be on “non-public” networks (out of a rough estimate of $100bn total). There are many variables here, but it is a significant value, especially since it implies considerable extra revenue pull-through in software, integration, maintenance and so on.
- As a cross reference, the enterprise Wi-Fi market is worth around $6bn per year and is mostly indoor-only. It is not unreasonable to imagine private cellular growing to a substantial fraction of that figure, especially given that Wi-Fi spending is often on upgrades rather than initial installs.
- Estimating the number of networks is hard, as some may be very small (e.g., a single store or ship), but managed in groups (a retail chain or shipping fleet). Others may be national-scale, such as private LTE / 5G networks deployed by utility companies. However, it is reasonable to think in terms of thousands and then tens of thousands over a five-year time horizon.

The main growth markets are expected to be:

- The US, where the CBRS ecosystem appears to have reached critical mass, with diverse use cases and large numbers of interested parties.
- Germany, where both large and mid-size manufacturing companies are keenly investigating private networks, with a roadmap to 5G and industrial automation. Initial deployments may be LTE-based, with 5G developments subject to thorough testing, evaluation and pilots – many of the potential users are quite conservative, and highly security-focused. MNOs are keen to be involved, but it remains to be seen how successful they can be.
- The UK, where the regulator has developed several highly innovative (and inexpensive) approaches to obtaining local spectrum.



- Japan, where numerous industrial companies and metropolitan authorities are keen to build out their own networks – and perhaps export the expertise as well.
- China is something of a special case, where government and state-owned enterprises can potentially get access to spectrum where needed. Though it is less likely to be a fully open market for any enterprise.
- Other European markets are likely to follow the early leads of Germany, UK or Netherlands models, although the French regulators seem to lean more towards MNO-centric approaches, except for the largest organisations like transport hubs and rail.

Relationship with other networks

Private LTE and 5G networks will not exist in a vacuum – most enterprises will maintain and grow various other connectivity platforms. A manufacturing campus will likely retain a large amount of direct fibre connectivity, Wi-Fi, and various proprietary wired and wireless technologies, for instance.

Some key trends are likely to be:

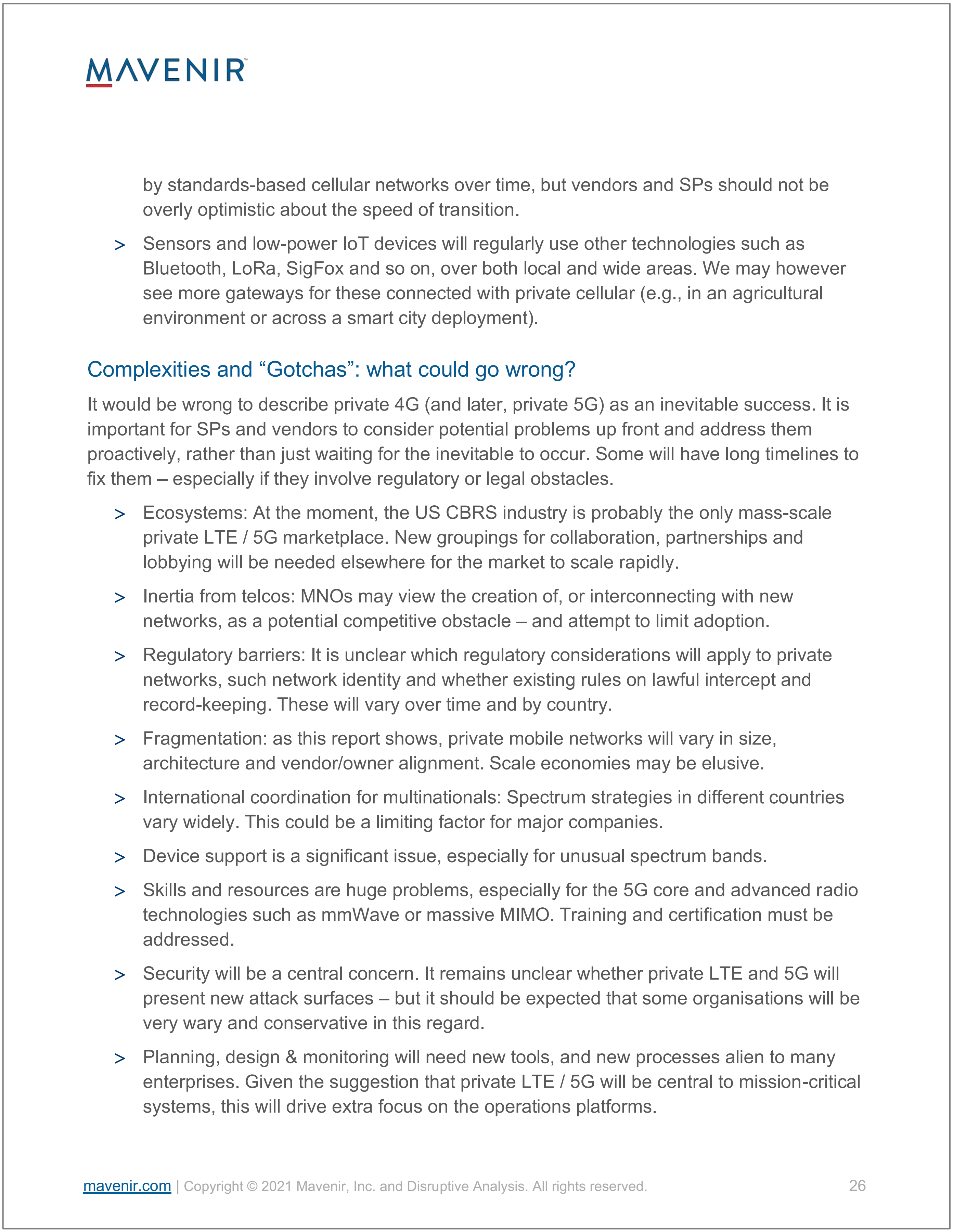
> The majority of deployments in 2020-2022 will be private 4G, not 5G. The true benefits of 5G (such as URLLC) will only emerge with the maturing of standalone 5G cores, which will need time for both products and expertise to hit the mass market.

> In theory, the same networks can service both private (enterprise) and public (MNO roaming /interconnect) use cases. In reality, we can expect many installations to have these isolated with a private overlay network. While seemingly "inefficient," this will ease conflicts around ownership and control – as well as liability in case of failure.

> Wi-Fi will not be generally displaced by private (or public) 4G or 5G, except in specific areas of overlap, with particular demanding applications involving mobility or IoT systems that cannot risk interference and network congestion. Anywhere where basic connectivity is needed for guests and visitors (e.g., hotels, shared office spaces), Wi-Fi will proliferate – and, with the advent of Wi-Fi6 – much more capable. In some cases, we will see integrated Wi-Fi + Private Cellular systems, although in others they will be kept separate.

> We can expect more focus over time on low-power/low-cost versions of private LTE, such as NB-IoT and LTE-M. At the moment, these tend to be lower priorities.

> In the industrial space, there are many niche and proprietary wireless technologies, often integrated with specific automation vendors' systems, and linked to deterministic networking, mesh-based resilience, and other features. These may start to be displaced



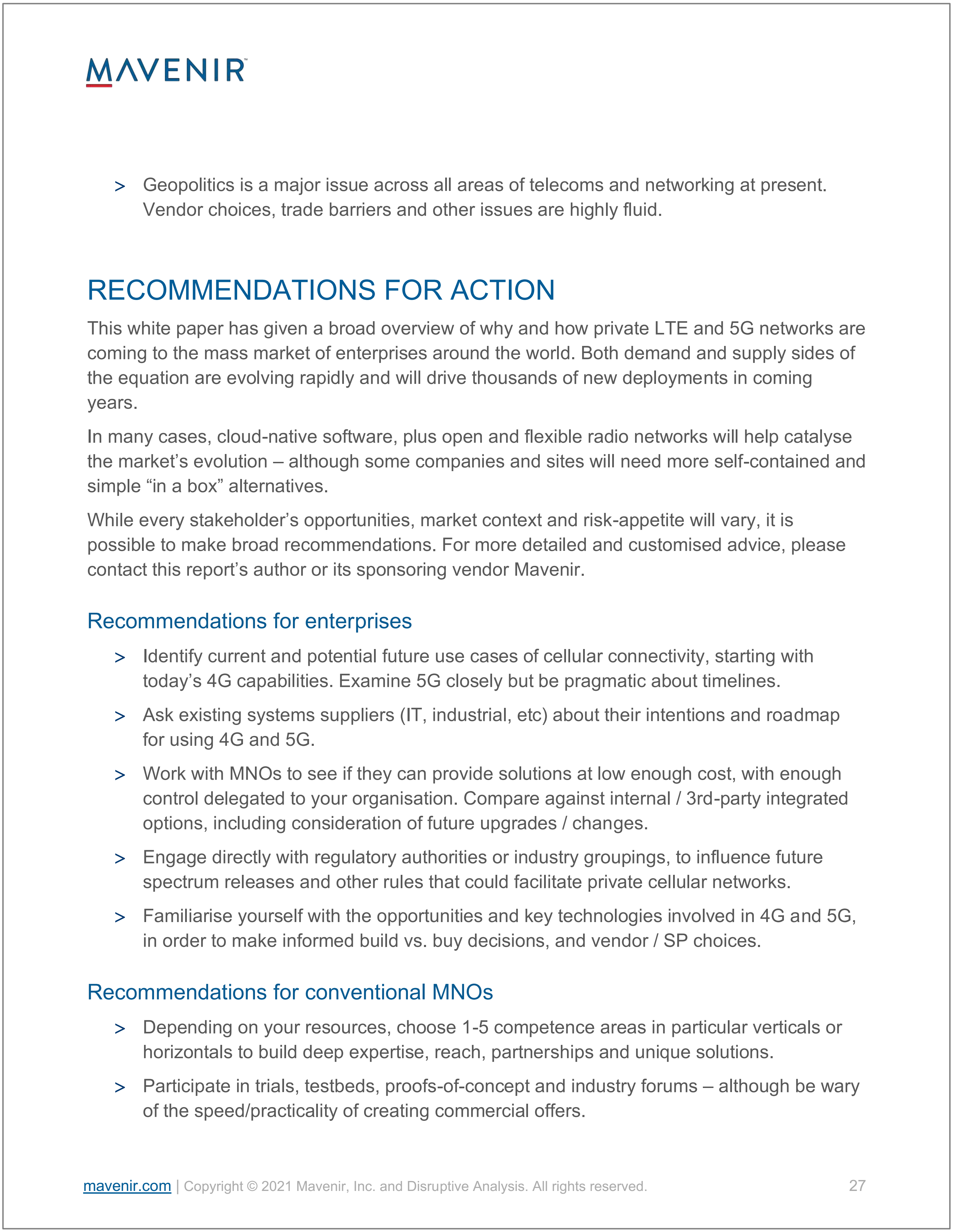
by standards-based cellular networks over time, but vendors and SPs should not be overly optimistic about the speed of transition.

- Sensors and low-power IoT devices will regularly use other technologies such as Bluetooth, LoRa, SigFox and so on, over both local and wide areas. We may however see more gateways for these connected with private cellular (e.g., in an agricultural environment or across a smart city deployment).

Complexities and "Gotchas": what could go wrong?

It would be wrong to describe private 4G (and later, private 5G) as an inevitable success. It is important for SPs and vendors to consider potential problems up front and address them proactively, rather than just waiting for the inevitable to occur. Some will have long timelines to fix them – especially if they involve regulatory or legal obstacles.

- Ecosystems: At the moment, the US CBRS industry is probably the only mass-scale private LTE / 5G marketplace. New groupings for collaboration, partnerships and lobbying will be needed elsewhere for the market to scale rapidly.
- Inertia from telcos: MNOs may view the creation of, or interconnecting with new networks, as a potential competitive obstacle – and attempt to limit adoption.
- Regulatory barriers: It is unclear which regulatory considerations will apply to private networks, such network identity and whether existing rules on lawful intercept and record-keeping. These will vary over time and by country.
- Fragmentation: as this report shows, private mobile networks will vary in size, architecture and vendor/owner alignment. Scale economies may be elusive.
- International coordination for multinationals: Spectrum strategies in different countries vary widely. This could be a limiting factor for major companies.
- Device support is a significant issue, especially for unusual spectrum bands.
- Skills and resources are huge problems, especially for the 5G core and advanced radio technologies such as mmWave or massive MIMO. Training and certification must be addressed.
- Security will be a central concern. It remains unclear whether private LTE and 5G will present new attack surfaces – but it should be expected that some organisations will be very wary and conservative in this regard.
- Planning, design & monitoring will need new tools, and new processes alien to many enterprises. Given the suggestion that private LTE / 5G will be central to mission-critical systems, this will drive extra focus on the operations platforms.



- Geopolitics is a major issue across all areas of telecoms and networking at present. Vendor choices, trade barriers and other issues are highly fluid.

RECOMMENDATIONS FOR ACTION

This white paper has given a broad overview of why and how private LTE and 5G networks are coming to the mass market of enterprises around the world. Both demand and supply sides of the equation are evolving rapidly and will drive thousands of new deployments in coming years.

In many cases, cloud-native software, plus open and flexible radio networks will help catalyse the market's evolution – although some companies and sites will need more self-contained and simple "in a box" alternatives.

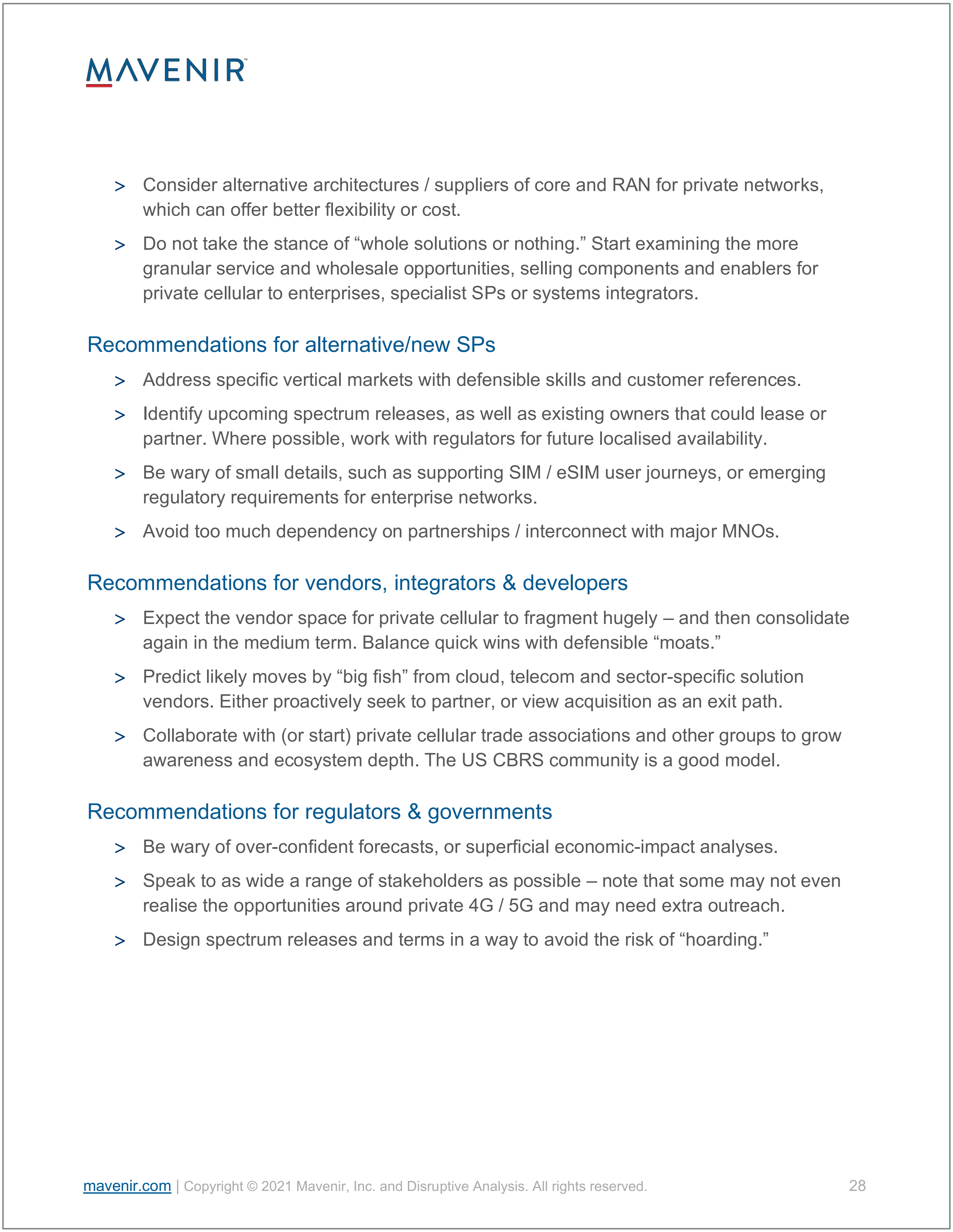
While every stakeholder's opportunities, market context and risk-appetite will vary, it is possible to make broad recommendations. For more detailed and customised advice, please contact this report's author or its sponsoring vendor Mavenir.

Recommendations for enterprises

- Identify current and potential future use cases of cellular connectivity, starting with today's 4G capabilities. Examine 5G closely but be pragmatic about timelines.
- Ask existing systems suppliers (IT, industrial, etc) about their intentions and roadmap for using 4G and 5G.
- Work with MNOs to see if they can provide solutions at low enough cost, with enough control delegated to your organisation. Compare against internal / 3rd-party integrated options, including consideration of future upgrades / changes.
- Engage directly with regulatory authorities or industry groupings, to influence future spectrum releases and other rules that could facilitate private cellular networks.
- Familiarise yourself with the opportunities and key technologies involved in 4G and 5G, in order to make informed build vs. buy decisions, and vendor / SP choices.

Recommendations for conventional MNOs

- Depending on your resources, choose 1-5 competence areas in particular verticals or horizontals to build deep expertise, reach, partnerships and unique solutions.
- Participate in trials, testbeds, proofs-of-concept and industry forums – although be wary of the speed/practicality of creating commercial offers.



MAVENIR

- Consider alternative architectures / suppliers of core and RAN for private networks, which can offer better flexibility or cost.
- Do not take the stance of "whole solutions or nothing." Start examining the more granular service and wholesale opportunities, selling components and enablers for private cellular to enterprises, specialist SPs or systems integrators.

Recommendations for alternative/new SPs

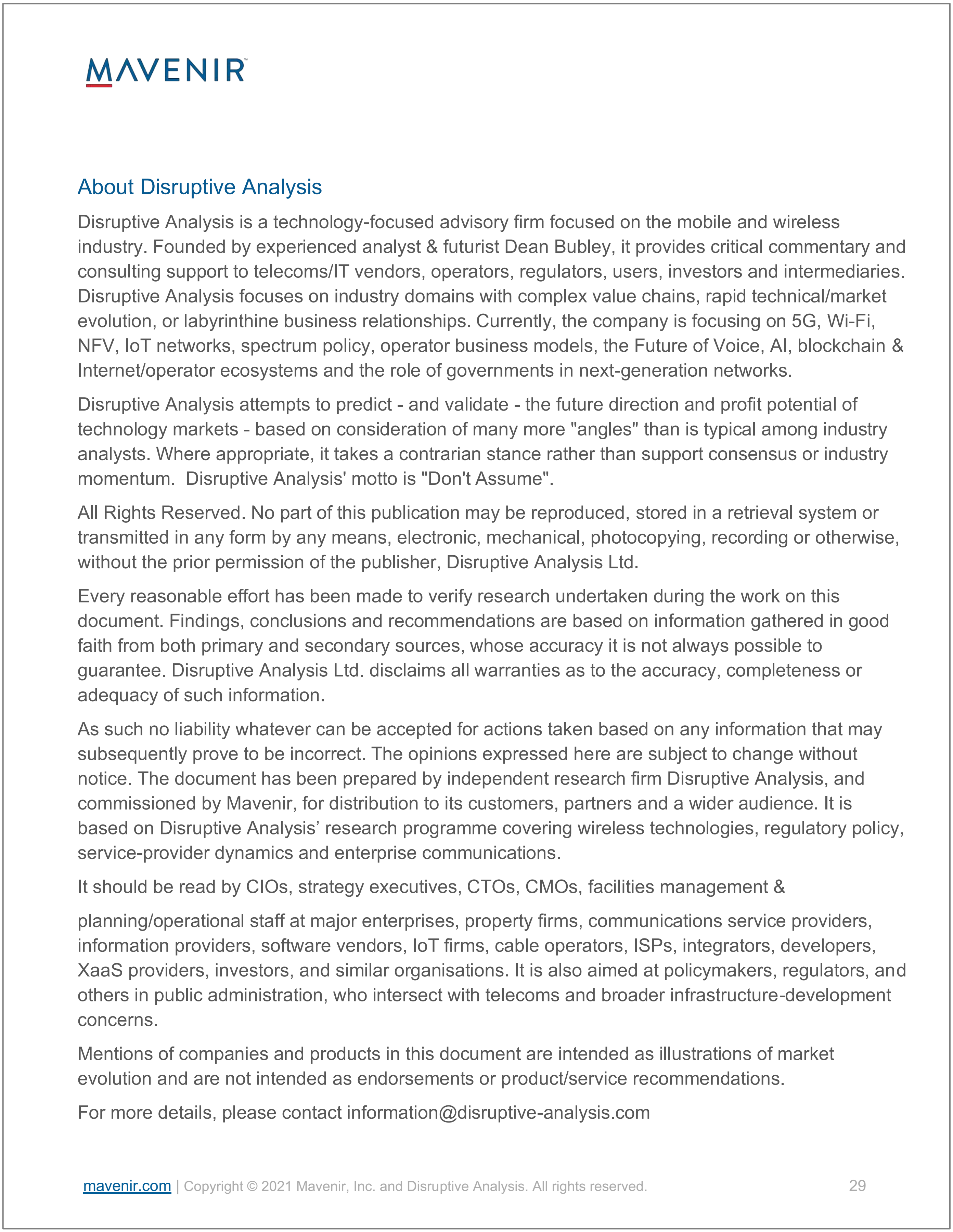
- Address specific vertical markets with defensible skills and customer references.
- Identify upcoming spectrum releases, as well as existing owners that could lease or partner. Where possible, work with regulators for future localised availability.
- Be wary of small details, such as supporting SIM / eSIM user journeys, or emerging regulatory requirements for enterprise networks.
- Avoid too much dependency on partnerships / interconnect with major MNOs.

Recommendations for vendors, integrators & developers

- Expect the vendor space for private cellular to fragment hugely – and then consolidate again in the medium term. Balance quick wins with defensible "moats."
- Predict likely moves by "big fish" from cloud, telecom and sector-specific solution vendors. Either proactively seek to partner, or view acquisition as an exit path.
- Collaborate with (or start) private cellular trade associations and other groups to grow awareness and ecosystem depth. The US CBRS community is a good model.

Recommendations for regulators & governments

- Be wary of over-confident forecasts, or superficial economic-impact analyses.
- Speak to as wide a range of stakeholders as possible – note that some may not even realise the opportunities around private 4G / 5G and may need extra outreach.
- Design spectrum releases and terms in a way to avoid the risk of "hoarding."



About Disruptive Analysis

Disruptive Analysis is a technology-focused advisory firm focused on the mobile and wireless industry. Founded by experienced analyst & futurist Dean Bubley, it provides critical commentary and consulting support to telecoms/IT vendors, operators, regulators, users, investors and intermediaries. Disruptive Analysis focuses on industry domains with complex value chains, rapid technical/market evolution, or labyrinthine business relationships. Currently, the company is focusing on 5G, Wi-Fi, NFV, IoT networks, spectrum policy, operator business models, the Future of Voice, AI, blockchain & Internet/operator ecosystems and the role of governments in next-generation networks.

Disruptive Analysis attempts to predict - and validate - the future direction and profit potential of technology markets - based on consideration of many more "angles" than is typical among industry analysts. Where appropriate, it takes a contrarian stance rather than support consensus or industry momentum. Disruptive Analysis' motto is "Don't Assume".

Every reasonable effort has been made to verify research undertaken during the work on this document. Findings, conclusions and recommendations are based on information gathered in good faith from both primary and secondary sources, whose accuracy it is not always possible to guarantee. Disruptive Analysis Ltd. disclaims all warranties as to the accuracy, completeness or adequacy of such information.

As such no liability whatever can be accepted for actions taken based on any information that may subsequently prove to be incorrect. The opinions expressed here are subject to change without notice. The document has been prepared by independent research firm Disruptive Analysis, and commissioned by Mavenir, for distribution to its customers, partners and a wider audience. It is based on Disruptive Analysis' research programme covering wireless technologies, regulatory policy, service-provider dynamics and enterprise communications.

It should be read by CIOs, strategy executives, CTOs, CMOs, facilities management &

planning/operational staff at major enterprises, property firms, communications service providers, information providers, software vendors, IoT firms, cable operators, ISPs, integrators, developers, XaaS providers, investors, and similar organisations. It is also aimed at policymakers, regulators, and others in public administration, who intersect with telecoms and broader infrastructure-development concerns.

Mentions of companies and products in this document are intended as illustrations of market evolution and are not intended as endorsements or product/service recommendations.

For more details, please contact information@disruptive-analysis.com

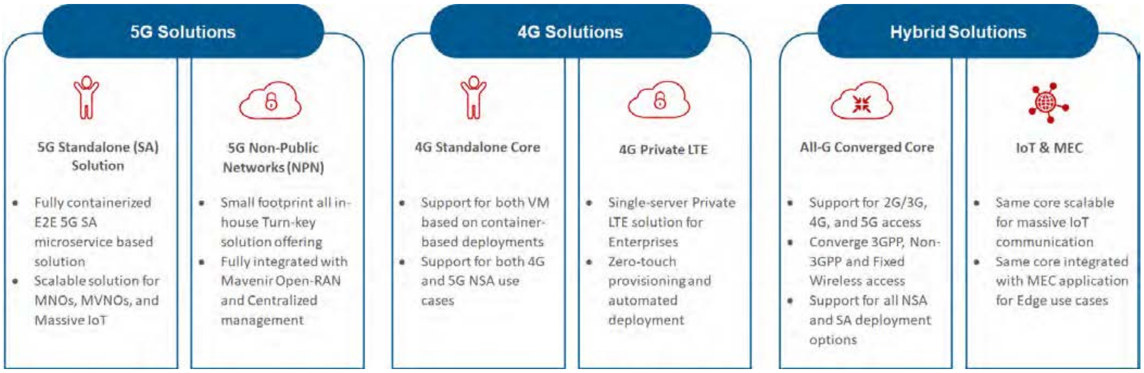
MAVENIR

SOLUTION BRIEF

Mavenir Converged Packet Core Solution

The Mavenir Converged Packet Core Solution is built with granular micro-services, following webscale principles that provide the required scalability, agility, and reliability in order to meet the wide range of use cases and stringent network performance requirements.

Mavenir's Converged Packet Core offers a comprehensive suite of End-to-End network functions for 2G/3G, 4G and 5G use cases. Solutions for mobile core networks can be tailored to fit customers' infrastructure requirements and business needs.



5G Solutions

5G Standalone (SA) Solution
- Fully containerized E2E 5G SA microservice based solution
- Scalable solution for MNOs, MVNOs, and Massive IoT

5G Non-Public Networks (NPN)
- Small footprint all in-house Turn-key solution offering
- Fully integrated with Mavenir Open-RAN and Centralized management

4G Solutions

4G Standalone Core
- Support for both VM based on container-based deployments
- Support for both 4G and 5G NSA use cases

4G Private LTE
- Single-server Private LTE solution for Enterprises
- Zero-touch provisioning and automated deployment

Hybrid Solutions

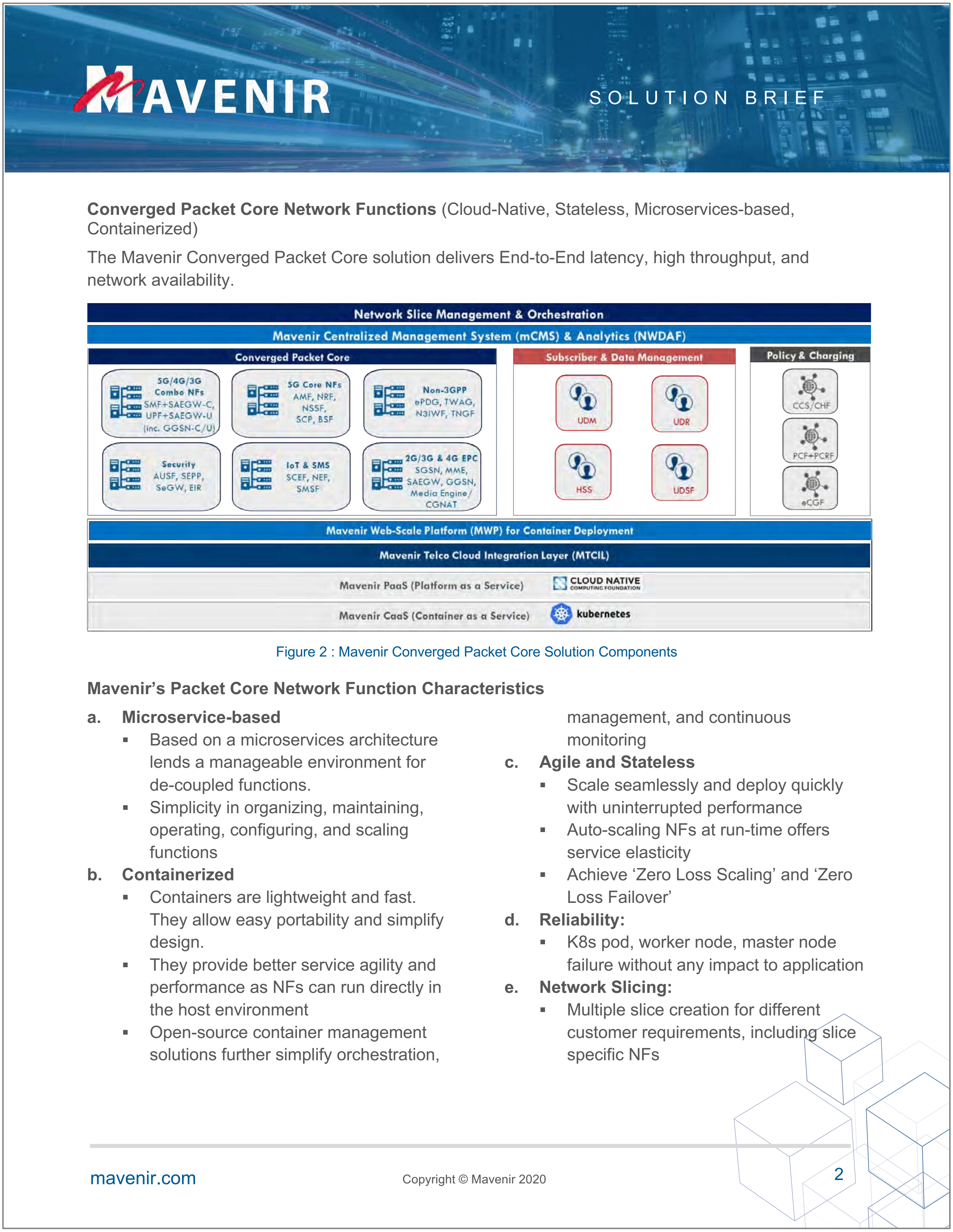
All-G Converged Core
- Support for 2G/3G, 4G, and 5G access
- Converge 3GPP, Non-3GPP and Fixed Wireless access
- Support for all NSA and SA deployment options

IoT & MEC
- Same core scalable for massive IoT communication
- Same core integrated with MEC application for Edge use cases

Figure 1 : Converged Packet Core Solution Offerings

Mavenir's 5G Core solution offers 5GC NF applications that are de-coupled and built independent of the platform, allowing the Mavenir 5GC NFs to run in any underlying CaaS/PaaS and IaaS layers. In addition, Mavenir has de-coupled the 5GC NF application services from the common management services to provide a truly disaggregated and independently scalable packet core architecture.

The Mavenir Converged Packet Core Solution provides an end-to-end fully containerized all in-house 5G Core Product Portfolio with Combo Nodes for 2G/3G and 4G support. In addition to multi-generation support, the Mavenir Web-Scaled Converged 5G Core also supports non-3GPP access.



MAVENIR

SOLUTION BRIEF

Converged Packet Core Network Functions (Cloud-Native, Stateless, Microservices-based, Containerized)

The Mavenir Converged Packet Core solution delivers End-to-End latency, high throughput, and network availability.

Network Slice Management & Orchestration
Mavenir Centralized Management System (mCMS) & Analytics (NWDAF)
Converged Packet Core
5G/4G/3G Combo NFs SMF+SAEGW-C, UPF+SAEGW-U (inc. GGSN-C/U)
5G Core NFs AMF, NRF, NSSF, SCP, BSF
Non-3GPP ePDG, TWAG, N3IWF, TNGF
Security AUSF, SEPP, SeGW, EIR
IoT & SMS SCEF, NEF, SMSF
2G/3G & 4G EPC SGSN, MME, SAEGW, GGSN, Media Engine/ CGNAT
Subscriber & Data Management
UDM
UDR
HSS
UDSF
Policy & Charging
CCS/CHF
PCF+PCRF
eCGF
Mavenir Web-Scale Platform (MWP) for Container Deployment
Mavenir Telco Cloud Integration Layer (MTCIL)
Mavenir PaaS (Platform as a Service)
CLOUD NATIVE COMPUTING FOUNDATION
Mavenir CaaS (Container as a Service)
kubernetes

Figure 2 : Mavenir Converged Packet Core Solution Components

Mavenir's Packet Core Network Function Characteristics

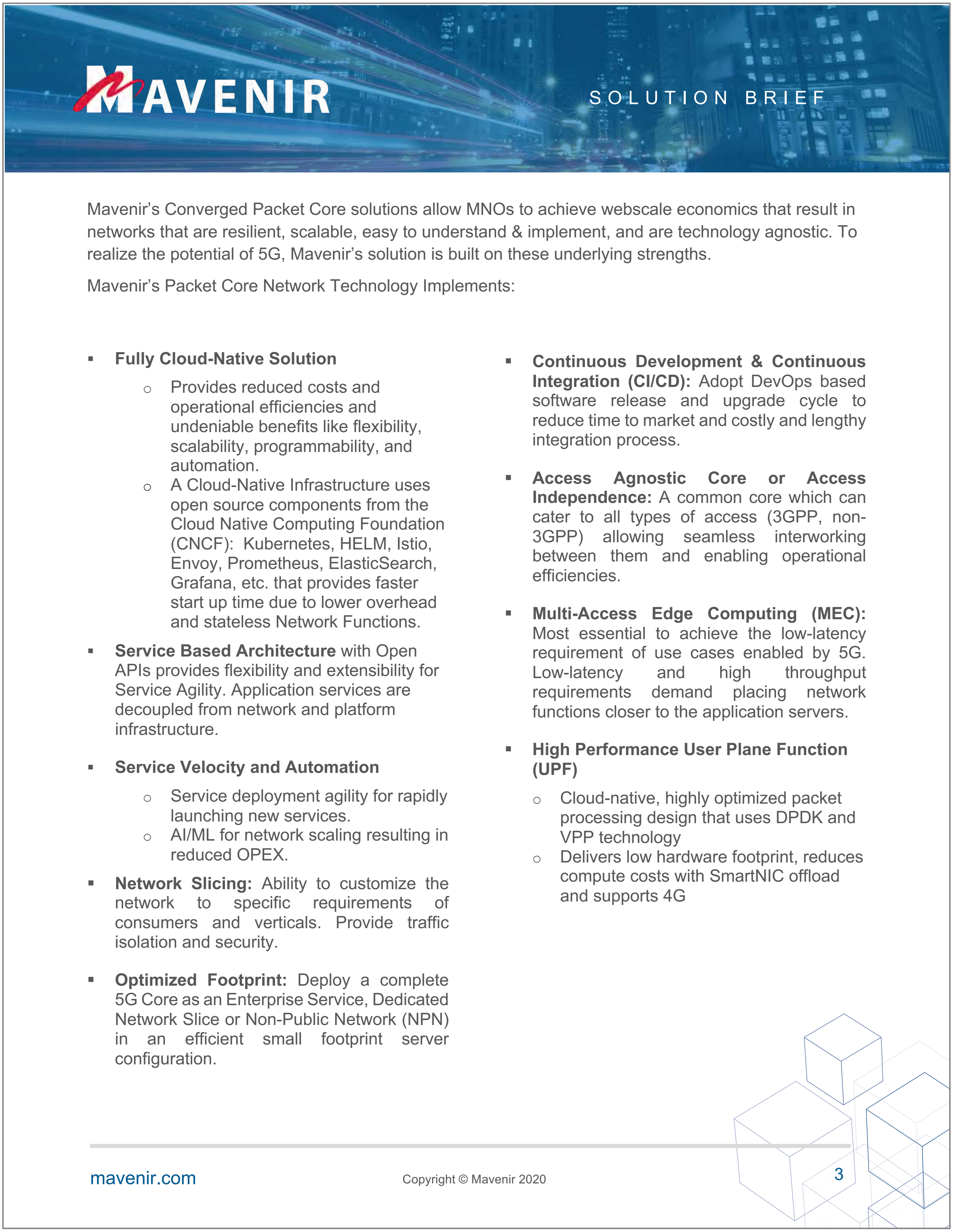
a. **Microservice-based**
   - Based on a microservices architecture lends a manageable environment for de-coupled functions.
   - Simplicity in organizing, maintaining, operating, configuring, and scaling functions

b. **Containerized**
   - Containers are lightweight and fast. They allow easy portability and simplify design.
   - They provide better service agility and performance as NFs can run directly in the host environment
   - Open-source container management solutions further simplify orchestration, management, and continuous monitoring

c. **Agile and Stateless**
   - Scale seamlessly and deploy quickly with uninterrupted performance
   - Auto-scaling NFs at run-time offers service elasticity
   - Achieve 'Zero Loss Scaling' and 'Zero Loss Failover'

d. **Reliability:**
   - K8s pod, worker node, master node failure without any impact to application

e. **Network Slicing:**
   - Multiple slice creation for different customer requirements, including slice specific NFs



MAVENIR

SOLUTION BRIEF

Mavenir's Converged Packet Core solutions allow MNOs to achieve webscale economics that result in networks that are resilient, scalable, easy to understand & implement, and are technology agnostic. To realize the potential of 5G, Mavenir's solution is built on these underlying strengths.

Mavenir's Packet Core Network Technology Implements:

- **Fully Cloud-Native Solution**
  - Provides reduced costs and operational efficiencies and undeniable benefits like flexibility, scalability, programmability, and automation.
  - A Cloud-Native Infrastructure uses open source components from the Cloud Native Computing Foundation (CNCF): Kubernetes, HELM, Istio, Envoy, Prometheus, ElasticSearch, Grafana, etc. that provides faster start up time due to lower overhead and stateless Network Functions.
- **Service Based Architecture** with Open APIs provides flexibility and extensibility for Service Agility. Application services are decoupled from network and platform infrastructure.
- **Service Velocity and Automation**
  - Service deployment agility for rapidly launching new services.
  - AI/ML for network scaling resulting in reduced OPEX.
- **Network Slicing:** Ability to customize the network to specific requirements of consumers and verticals. Provide traffic isolation and security.
- **Optimized Footprint:** Deploy a complete 5G Core as an Enterprise Service, Dedicated Network Slice or Non-Public Network (NPN) in an efficient small footprint server configuration.
- **Continuous Development & Continuous Integration (CI/CD):** Adopt DevOps based software release and upgrade cycle to reduce time to market and costly and lengthy integration process.
- **Access Agnostic Core or Access Independence:** A common core which can cater to all types of access (3GPP, non-3GPP) allowing seamless interworking between them and enabling operational efficiencies.
- **Multi-Access Edge Computing (MEC):** Most essential to achieve the low-latency requirement of use cases enabled by 5G. Low-latency and high throughput requirements demand placing network functions closer to the application servers.
- **High Performance User Plane Function (UPF)**
  - Cloud-native, highly optimized packet processing design that uses DPDK and VPP technology
  - Delivers low hardware footprint, reduces compute costs with SmartNIC offload and supports 4G

Cloud native infrastructure and its benefits

Mavenir offers flexibility to operators and enterprises with a multi-cloud environment, allowing usage of resources based on an organizations' end goals. Mavenir's 5G Core can run on any public, private or hybrid cloud.

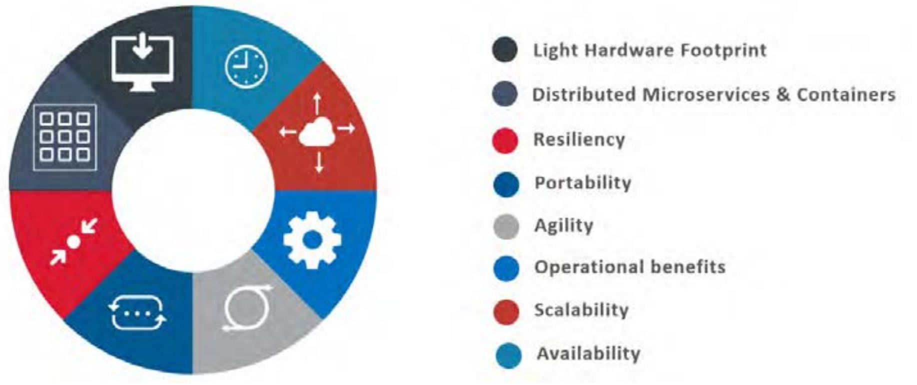
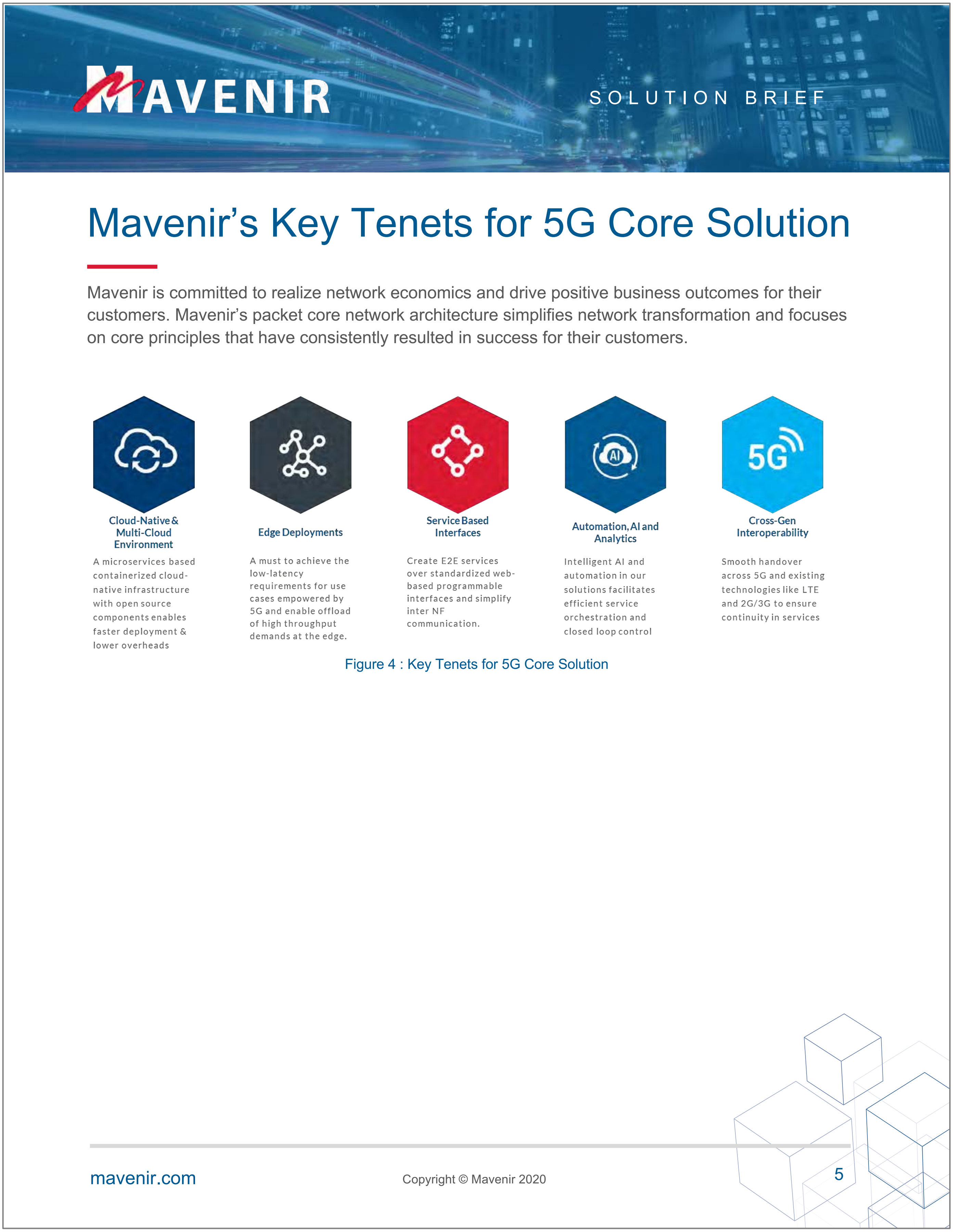


Figure 3 : Benefits of a cloud-native infrastructure

Benefits of a cloud-native infrastructure

a. Meets specific business requirements
b. Reduces Operational Costs
    - Changes in demand can be handled more easily, scaling IT capacity up or down as needed
    - Applications can be shifted between clouds to eliminate resource redundancy and reduce operational costs
c. Prevents downtime with redundancy and high availability
d. Mitigates vendor lock-in
    - Loosely coupled components support portability.
    - Mavenir's deployment strategy and CI/CD assists in reducing dependency on a single cloud vendor. MNOs can leverage competitive pricing and features offered by cloud providers
e. Provides an NFVI agnostic architecture at lowest TCO



MAVENIR

SOLUTION BRIEF

Mavenir's Key Tenets for 5G Core Solution

Mavenir is committed to realize network economics and drive positive business outcomes for their customers. Mavenir's packet core network architecture simplifies network transformation and focuses on core principles that have consistently resulted in success for their customers.

Cloud-Native & Multi-Cloud Environment

A microservices based containerized cloud-native infrastructure with open source components enables faster deployment & lower overheads

Edge Deployments

A must to achieve the low-latency requirements for use cases empowered by 5G and enable offload of high throughput demands at the edge.

Service Based Interfaces

Create E2E services over standardized web-based programmable interfaces and simplify inter NF communication.

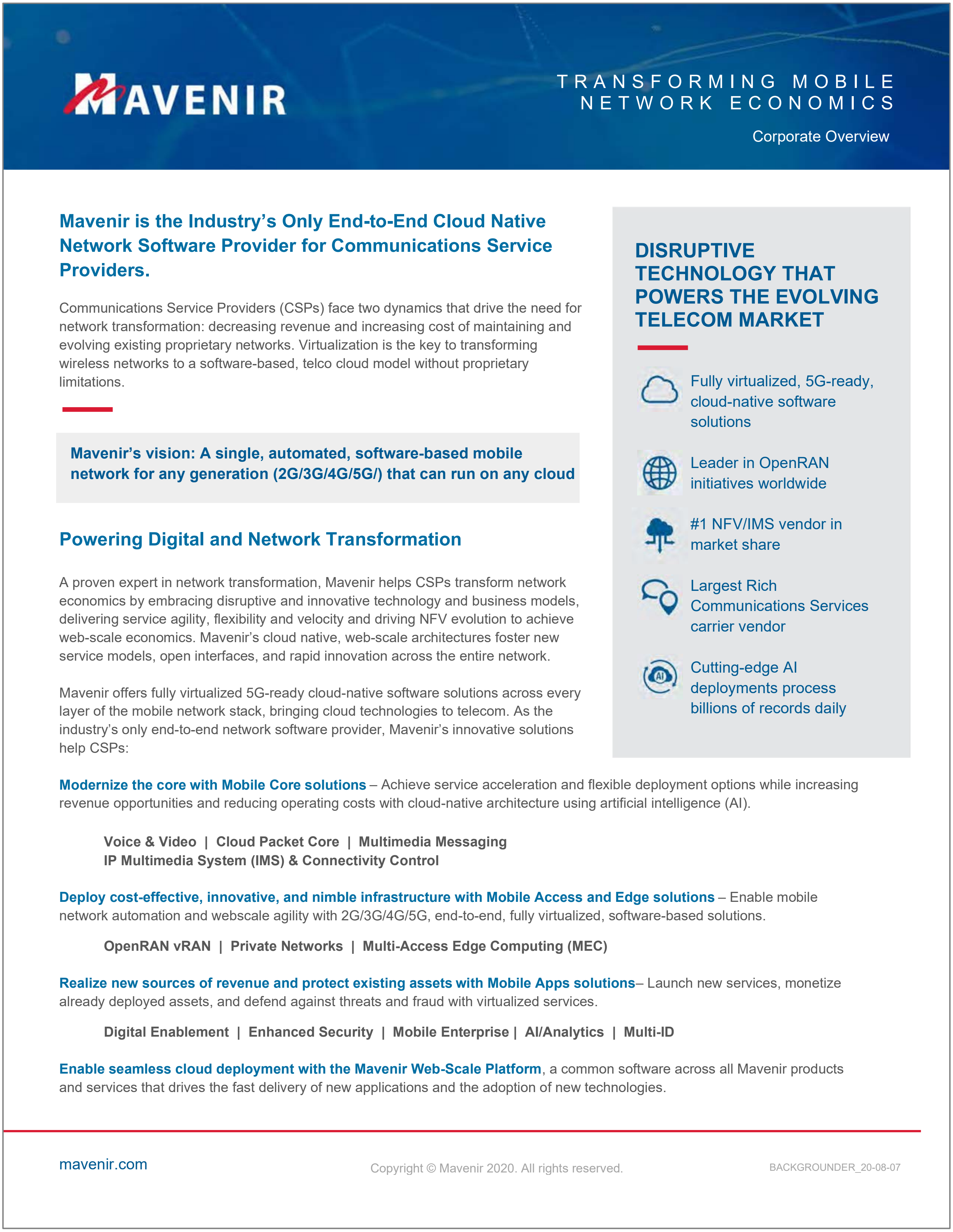
Automation, AI and Analytics

Intelligent AI and automation in our solutions facilitates efficient service orchestration and closed loop control

Cross-Gen Interoperability

Smooth handover across 5G and existing technologies like LTE and 2G/3G to ensure continuity in services

Figure 4 : Key Tenets for 5G Core Solution



MAVENIR

TRANSFORMING MOBILE NETWORK ECONOMICS

Corporate Overview

Mavenir is the Industry’s Only End-to-End Cloud Native Network Software Provider for Communications Service Providers.

Communications Service Providers (CSPs) face two dynamics that drive the need for network transformation: decreasing revenue and increasing cost of maintaining and evolving existing proprietary networks. Virtualization is the key to transforming wireless networks to a software-based, telco cloud model without proprietary limitations.

Mavenir’s vision: A single, automated, software-based mobile network for any generation (2G/3G/4G/5G/) that can run on any cloud

Powering Digital and Network Transformation

A proven expert in network transformation, Mavenir helps CSPs transform network economics by embracing disruptive and innovative technology and business models, delivering service agility, flexibility and velocity and driving NFV evolution to achieve web-scale economics. Mavenir’s cloud native, web-scale architectures foster new service models, open interfaces, and rapid innovation across the entire network.

Mavenir offers fully virtualized 5G-ready cloud-native software solutions across every layer of the mobile network stack, bringing cloud technologies to telecom. As the industry’s only end-to-end network software provider, Mavenir’s innovative solutions help CSPs:

DISRUPTIVE TECHNOLOGY THAT POWERS THE EVOLVING TELECOM MARKET

- Fully virtualized, 5G-ready, cloud-native software solutions
- Leader in OpenRAN initiatives worldwide
- #1 NFV/IMS vendor in market share
- Largest Rich Communications Services carrier vendor
- Cutting-edge AI deployments process billions of records daily

Modernize the core with Mobile Core solutions – Achieve service acceleration and flexible deployment options while increasing revenue opportunities and reducing operating costs with cloud-native architecture using artificial intelligence (AI).

Voice & Video | Cloud Packet Core | Multimedia Messaging
IP Multimedia System (IMS) & Connectivity Control

Deploy cost-effective, innovative, and nimble infrastructure with Mobile Access and Edge solutions – Enable mobile network automation and webscale agility with 2G/3G/4G/5G, end-to-end, fully virtualized, software-based solutions.

OpenRAN vRAN | Private Networks | Multi-Access Edge Computing (MEC)

Realize new sources of revenue and protect existing assets with Mobile Apps solutions– Launch new services, monetize already deployed assets, and defend against threats and fraud with virtualized services.

Digital Enablement | Enhanced Security | Mobile Enterprise | AI/Analytics | Multi-ID

Enable seamless cloud deployment with the Mavenir Web-Scale Platform, a common software across all Mavenir products and services that drives the fast delivery of new applications and the adoption of new technologies.

mavenir.com

BACKGROUNDER_20-08-07

MAVENIR AT-A-GLANCE

WORLD'S **#1** MESSAGING PROVIDER

#1 NFV/IMS
MARKET SHARE VENDOR

4 Billion
SUBSCIBERS SUPPORTED GLOBALLY

250 Global MNO
CUSTOMERS

US-Based HQ

17 of Top 20
OPERATORS GLOBALLY

Global Force
4200+ EMPLOYEES
60% R&D / INNOVATION
>$500M REVENUE

AVERAGE CUSTOMER RELATIONSHIP
of Over 12 Years

WHY MAVENIR?

Innovator and Leader

Mavenir leverages experience and expertise in virtualization, automation and cloudification to deliver solutions for next-generation networks. Mavenir supports ***interoperability with every major product and vendor***.

Global Tier 1 Operators are Mavenir Customers

Mavenir's customer base of more than 250 global MNOs includes:

T-Mobile · verizon · Telefonica · Deutsche Telekom
AT&T · dish · SFR · vodafone
Bell · ROGERS · Partner · TIM
Rakuten · TURKCELL · airtel · VEON
orange · O2 · اتصالات etisalat · BSNL
TELKOMSEL

MAVENIR RECOGNIZED FOR INDUSTRY FIRSTS AND AWARDS ACROSS ENTIRE PORTFOLIO OF SOLUTIONS*: MOBILE CORE | MOBILE ACCESS | MOBILE SERVICES

LEARN MORE AND CONTACT US AT MAVENIR.COM

*VOLTE DEPLOYMENT – GLOBAL, VOLTE DEPLOYMENT – UK, VOLTE DEPLOYMENT – GERMANY (AT SCALE), RCS DEPLOYMENT – USA, VIRTUALIZED VOLTE DEPLOYMENT (AT SCALE)
2020 5G WORLD AWARDS - BEST OPENRAN TECHNOLOGY, 2020 5G WORLD AWARDS - BEST 5G CORE TECHNOLOGY, 2017 COMMUNICATIONS SOLUTIONS AWARDS - PRODUCT OF THE YEAR FOR RCS CLOUD PLATFORM, 2017 LTE VOICE AWARDS - BEST USE OF VOLTE NETWORK POST COMMERCIALIZATION, WINNER, "BEST RAN PRODUCT," 2018 TECHXLR8 ASIA AWARDS.

mavenir.com

BACKGROUNDER_20-08-07

Open RAN Integration: *Run With It*

White Paper
First Quarter 2021

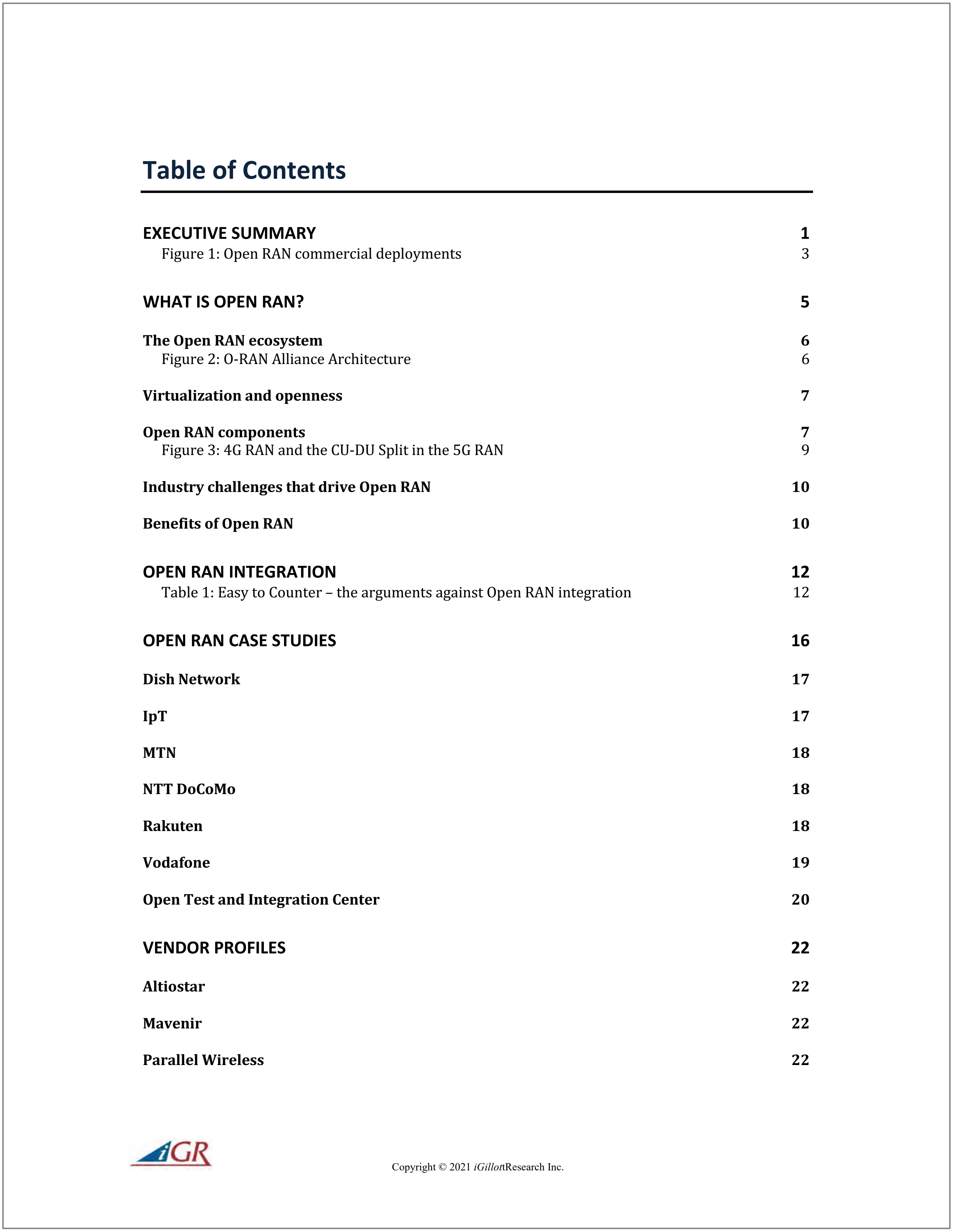
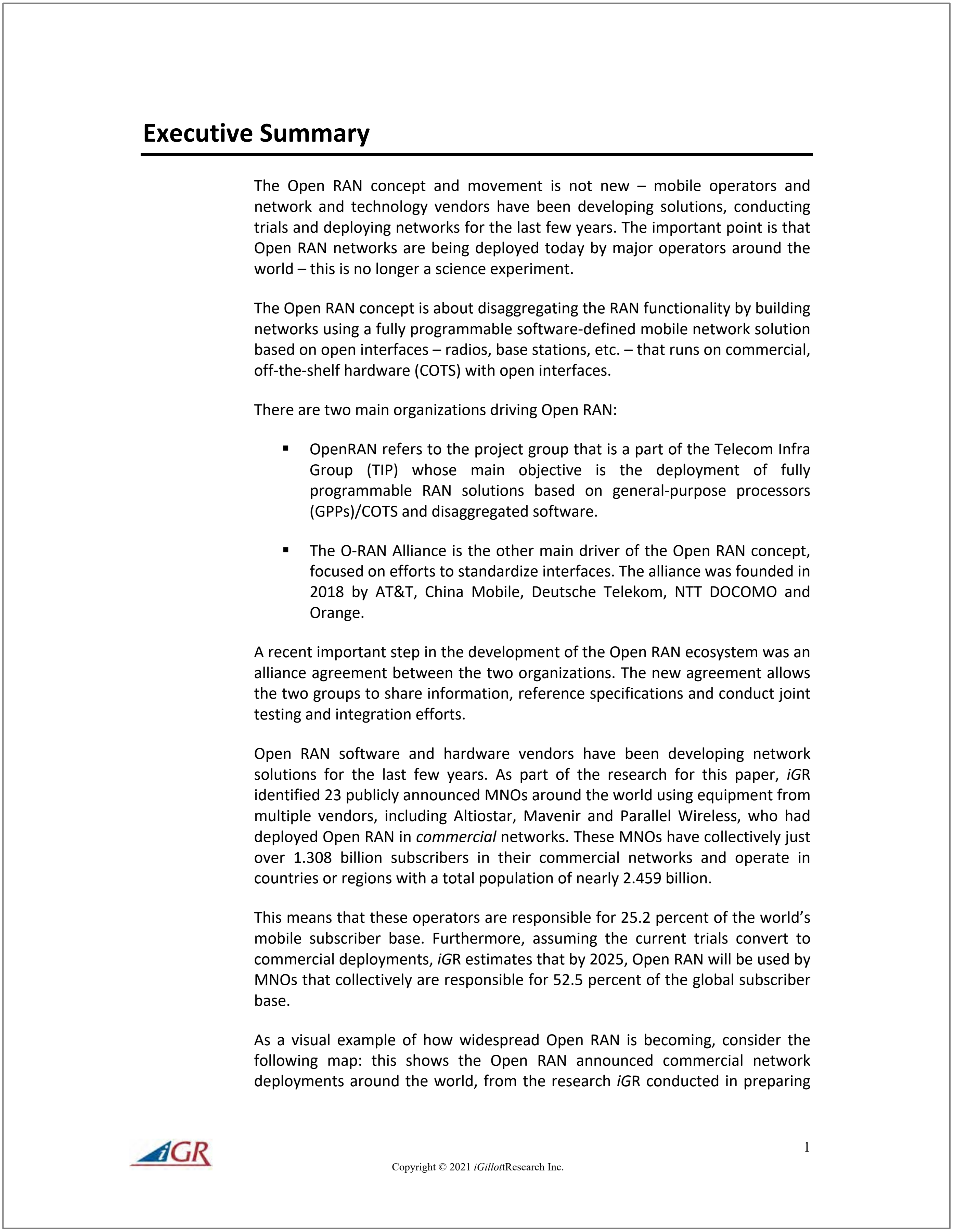


Table of Contents



Executive Summary

The Open RAN concept and movement is not new – mobile operators and network and technology vendors have been developing solutions, conducting trials and deploying networks for the last few years. The important point is that Open RAN networks are being deployed today by major operators around the world – this is no longer a science experiment.

The Open RAN concept is about disaggregating the RAN functionality by building networks using a fully programmable software-defined mobile network solution based on open interfaces – radios, base stations, etc. – that runs on commercial, off-the-shelf hardware (COTS) with open interfaces.

There are two main organizations driving Open RAN:

- OpenRAN refers to the project group that is a part of the Telecom Infra Group (TIP) whose main objective is the deployment of fully programmable RAN solutions based on general-purpose processors (GPPs)/COTS and disaggregated software.

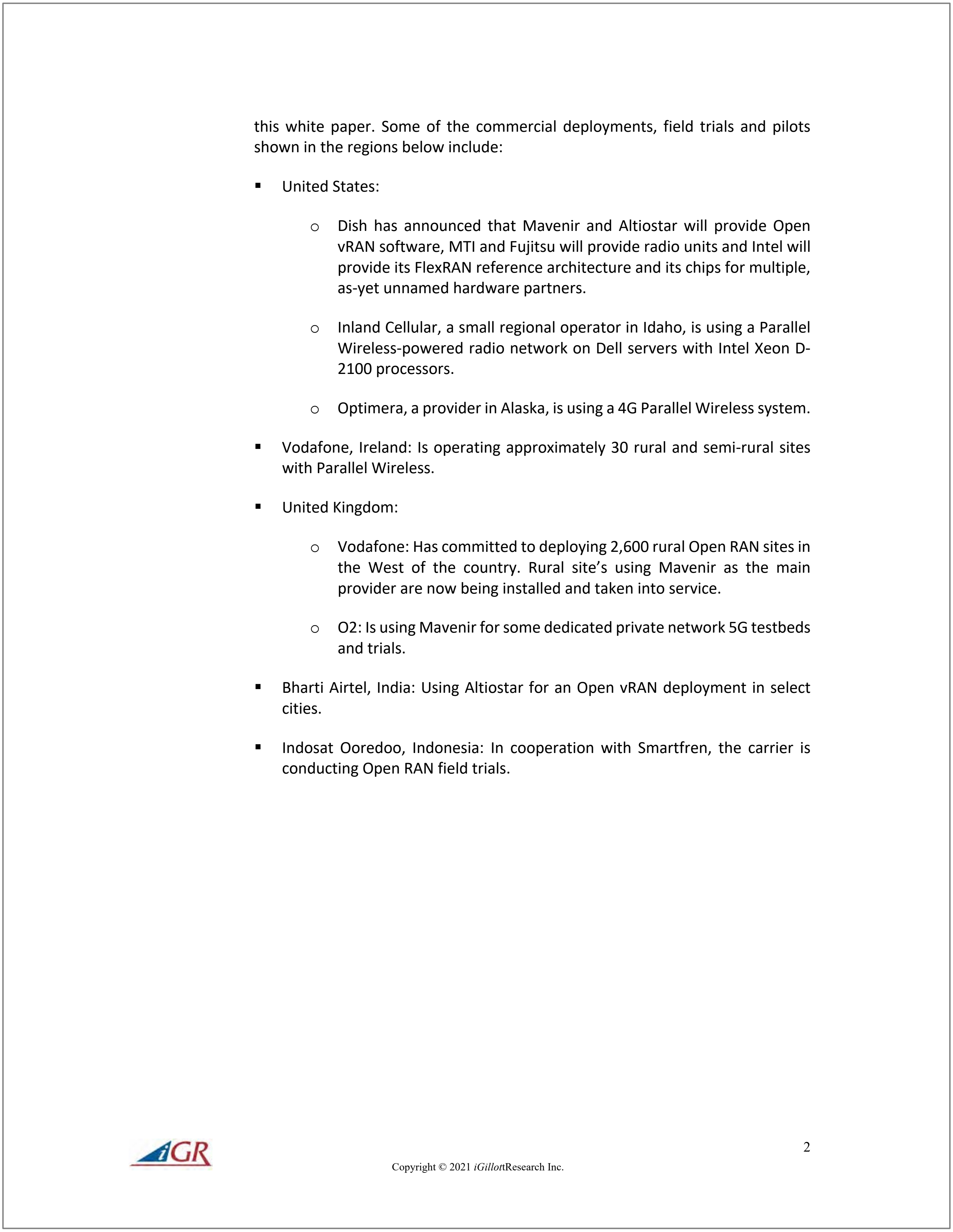
- The O-RAN Alliance is the other main driver of the Open RAN concept, focused on efforts to standardize interfaces. The alliance was founded in 2018 by AT&T, China Mobile, Deutsche Telekom, NTT DOCOMO and Orange.

A recent important step in the development of the Open RAN ecosystem was an alliance agreement between the two organizations. The new agreement allows the two groups to share information, reference specifications and conduct joint testing and integration efforts.

Open RAN software and hardware vendors have been developing network solutions for the last few years. As part of the research for this paper, *iG*R identified 23 publicly announced MNOs around the world using equipment from multiple vendors, including Altiostar, Mavenir and Parallel Wireless, who had deployed Open RAN in *commercial* networks. These MNOs have collectively just over 1.308 billion subscribers in their commercial networks and operate in countries or regions with a total population of nearly 2.459 billion.

This means that these operators are responsible for 25.2 percent of the world's mobile subscriber base. Furthermore, assuming the current trials convert to commercial deployments, *iG*R estimates that by 2025, Open RAN will be used by MNOs that collectively are responsible for 52.5 percent of the global subscriber base.

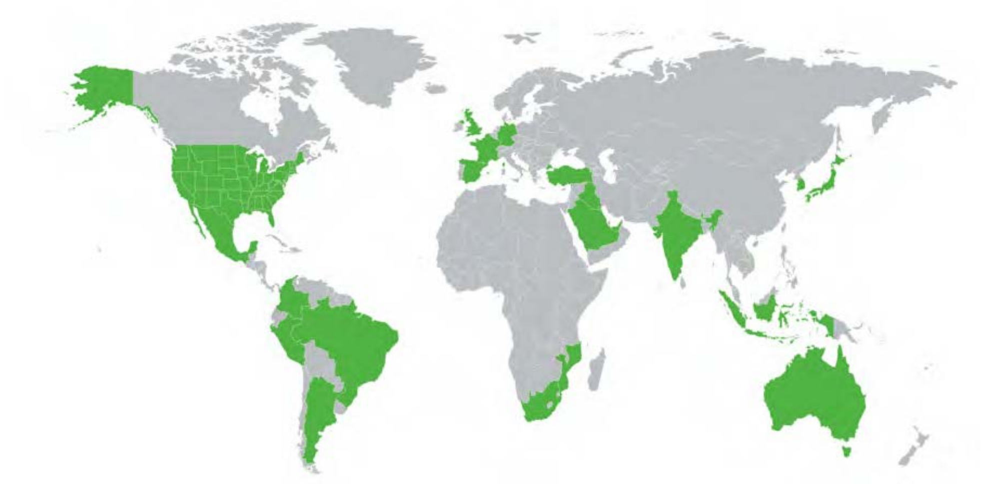
As a visual example of how widespread Open RAN is becoming, consider the following map: this shows the Open RAN announced commercial network deployments around the world, from the research *iG*R conducted in preparing



this white paper. Some of the commercial deployments, field trials and pilots shown in the regions below include:

- United States:
  - Dish has announced that Mavenir and Altiostar will provide Open vRAN software, MTI and Fujitsu will provide radio units and Intel will provide its FlexRAN reference architecture and its chips for multiple, as-yet unnamed hardware partners.
  - Inland Cellular, a small regional operator in Idaho, is using a Parallel Wireless-powered radio network on Dell servers with Intel Xeon D-2100 processors.
  - Optimera, a provider in Alaska, is using a 4G Parallel Wireless system.
- Vodafone, Ireland: Is operating approximately 30 rural and semi-rural sites with Parallel Wireless.
- United Kingdom:
  - Vodafone: Has committed to deploying 2,600 rural Open RAN sites in the West of the country. Rural site's using Mavenir as the main provider are now being installed and taken into service.
  - O2: Is using Mavenir for some dedicated private network 5G testbeds and trials.
- Bharti Airtel, India: Using Altiostar for an Open vRAN deployment in select cities.
- Indosat Ooredoo, Indonesia: In cooperation with Smartfren, the carrier is conducting Open RAN field trials.

Figure 1: Open RAN commercial deployments



Source: *iG*R; company reports; 2021

Clearly, Open RAN is no longer a regional solution, nor one that only applies to greenfield operators or MNOs in developing regions of the world. Open RAN has been deployed to support legacy 2G and 3G network technologies, as well as 4G LTE and 5G. It has been deployed in the most developed and competitive markets in the world, supporting some of the fastest growing regions.

These MNOs have realized significant savings in CapEx and OpEx and many have discussed this publicly. The benefits of deploying Open RAN are real. Consider:

- Accenture stated that 5G deployments that used COTS hardware and Open RAN software had seen CapEx savings of 49 percent compared to traditional deployment options.
- Senza Fili estimated the savings for a cloud RAN deployment to be 37 percent over five years, compared to a DRAN deployment. Specifically, the study showed a 49 percent savings in CapEx in year one and a cumulative 31 percent savings in OpEx over the five years.
- Strategy Analytics modelled the TCO of Open RAN over a five-year period. This model showed 40 percent lower CapEx and 34 percent lower OpEx compared to a legacy RAN.

Vodafone shared network performance information from its OpenRAN deployment in Turkey. Vodafone stated that the network has achieved 96 KPIs in both 2G and 4G networks; achieved QoS levels that are already acceptable (as of October 2019); and that, as of October 2019, that network optimization was ongoing, and they expected to achieve all of the target KPIs soon. And in April

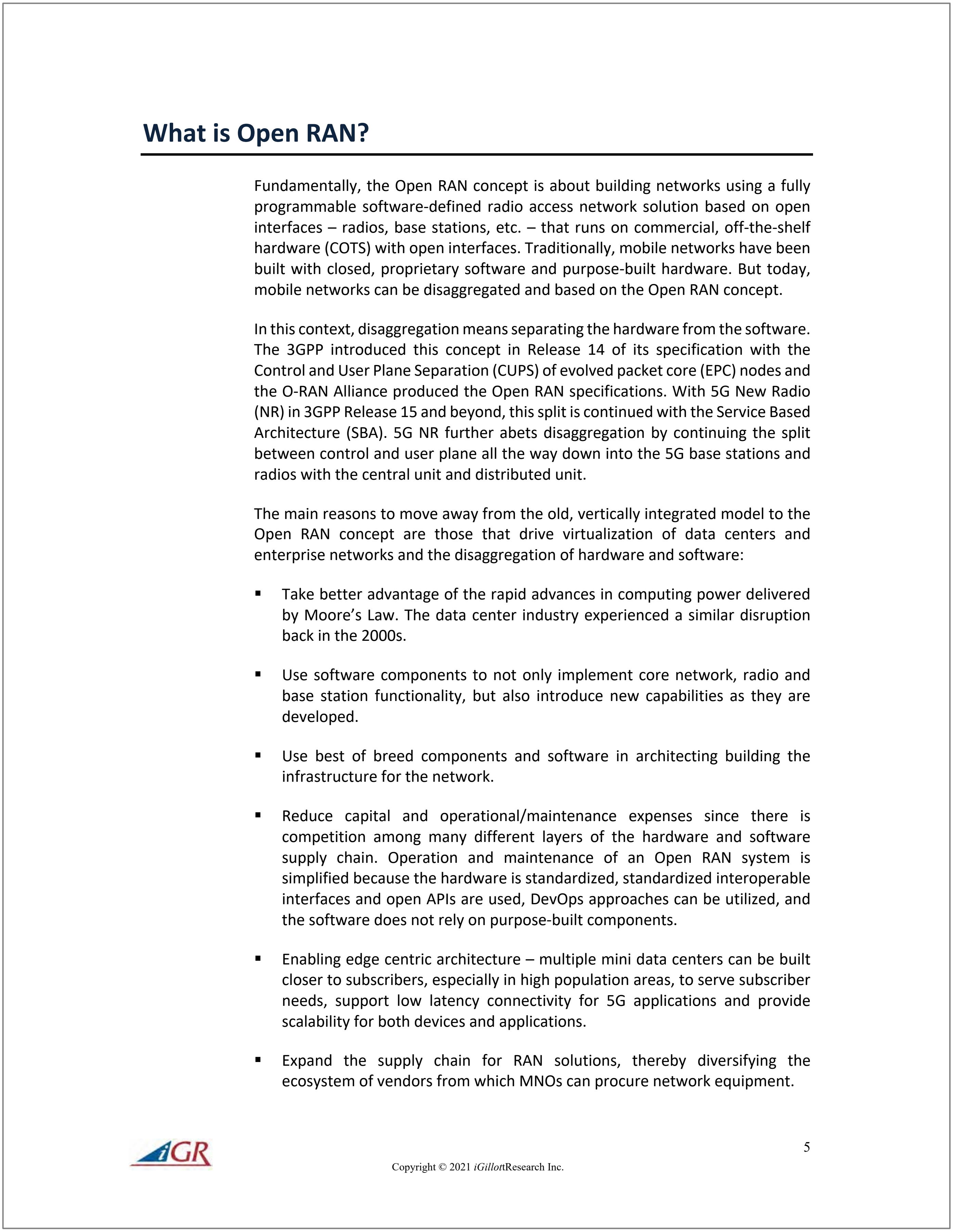
2020, Vodafone Idea announced that OpenRAN has been deployed on multiple cell sites and has been carrying commercial traffic since December 2019.

Rakuten is a textbook example of how Open RAN can support a nationwide mobile operator. In 2019, the Japanese carrier was the first to implement a multi-vendor RAN, using products from Altiostar, Airspan, Mavenir, Nokia and others. Nokia opened their radio interfaces to Altiostar's BBU which was running on a Cisco virtualization platform. Other functions within the network were also multi-vendor such as the EPC from Cisco, and IMS and RCS applications from Mavenir. Rakuten's network began as an LTE network consisting of both macro and small cells. The company has since evolved its network to 5G NR in 2020.

In April 2020, Dish Network announced the first vendor selection for its 5G Open RAN nationwide network deployment, using spectrum Dish has acquired over the last few years. To date, Dish has announced several vendors for its Open RAN network, including Mavenir, Altiostar, MTI, Qualcomm, Intel, and Fujitsu.

This shows how cloud, virtualization, openness and vRAN architectures and practices can be applied to a new network deployment. With Rakuten, a legacy vendor opened their interfaces to support Open RAN radios and baseband units from other vendors. Rakuten's CTO Tareq Amin has said the Open RAN framework has proved approximately 40 percent less expensive than traditional telecommunications infrastructure (Source: Light Reading; SDX Central, 2020). According to press reports, Rakuten deployed lean cell sites, with only antenna and remote radio heads, easing site acquisition and reducing deployment costs, and uses virtual RAN (vRAN) for baseband processing.

The takeaway here is that Open RAN is real; Open RAN can be, and is being, deployed in commercial networks today; the Open RAN community is coalescing and coordinating to move deployments along; the cost savings are being realized; and operational performance requirements and KPIs are being met.



What is Open RAN?

Fundamentally, the Open RAN concept is about building networks using a fully programmable software-defined radio access network solution based on open interfaces – radios, base stations, etc. – that runs on commercial, off-the-shelf hardware (COTS) with open interfaces. Traditionally, mobile networks have been built with closed, proprietary software and purpose-built hardware. But today, mobile networks can be disaggregated and based on the Open RAN concept.

In this context, disaggregation means separating the hardware from the software. The 3GPP introduced this concept in Release 14 of its specification with the Control and User Plane Separation (CUPS) of evolved packet core (EPC) nodes and the O-RAN Alliance produced the Open RAN specifications. With 5G New Radio (NR) in 3GPP Release 15 and beyond, this split is continued with the Service Based Architecture (SBA). 5G NR further abets disaggregation by continuing the split between control and user plane all the way down into the 5G base stations and radios with the central unit and distributed unit.

The main reasons to move away from the old, vertically integrated model to the Open RAN concept are those that drive virtualization of data centers and enterprise networks and the disaggregation of hardware and software:

- Take better advantage of the rapid advances in computing power delivered by Moore's Law. The data center industry experienced a similar disruption back in the 2000s.
- Use software components to not only implement core network, radio and base station functionality, but also introduce new capabilities as they are developed.
- Use best of breed components and software in architecting building the infrastructure for the network.
- Reduce capital and operational/maintenance expenses since there is competition among many different layers of the hardware and software supply chain. Operation and maintenance of an Open RAN system is simplified because the hardware is standardized, standardized interoperable interfaces and open APIs are used, DevOps approaches can be utilized, and the software does not rely on purpose-built components.
- Enabling edge centric architecture – multiple mini data centers can be built closer to subscribers, especially in high population areas, to serve subscriber needs, support low latency connectivity for 5G applications and provide scalability for both devices and applications.
- Expand the supply chain for RAN solutions, thereby diversifying the ecosystem of vendors from which MNOs can procure network equipment.

The Open RAN ecosystem

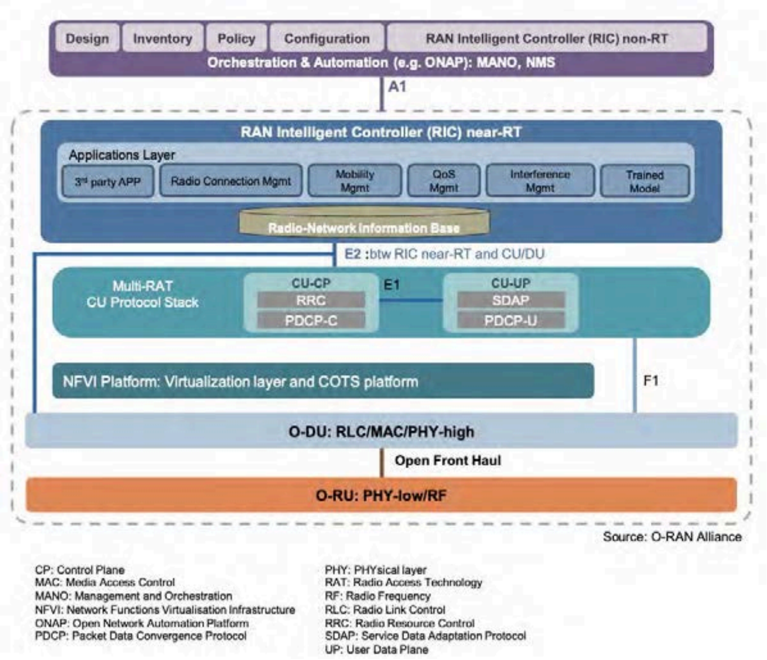
There are two main organizations driving Open RAN movement:

- OpenRAN refers to the project group that is a part of the Telecom Infra Group (TIP). The main objective is the deployment of fully programmable RAN solutions based on GPPP/COTS and disaggregated software so that operators and vendors can benefit from the flexibility and faster pace of innovation capable with software-driven development.

- The O-RAN Alliance is the other main driver of the OpenRAN concept, especially the efforts to standardize interfaces, in addition to the TIP. Founded in 2018 by AT&T, China Mobile, Deutsche Telekom, NTT DOCOMO and Orange, the O-RAN Alliance's goal is to foster the development of reference designs and standards such that current and future RANs can be built with "virtualized network elements, white-box hardware and standardized interfaces that fully embrace O-RAN's core principles of intelligence and openness." (Note: The O-RAN Alliance was created by merging the C-RAN Alliance and the xRAN Forum.)

The following graphic summarizes the components of the O-RAN Alliance's reference architecture.

Figure 2: O-RAN Alliance Architecture


Design
Inventory
Policy
Configuration
RAN Intelligent Controller (RIC) non-RT
Orchestration & Automation (e.g. ONAP): MANO, NMS
A1
RAN Intelligent Controller (RIC) near-RT
Applications Layer
3rd party APP
Radio Connection Mgmt
Mobility Mgmt
QoS Mgmt
Interference Mgmt
Trained Model
Radio-Network Information Base
E2 :btw RIC near-RT and CU/DU
Multi-RAT CU Protocol Stack
CU-CP
RRC
PDCP-C
E1
CU-UP
SDAP
PDCP-U
NFVI Platform: Virtualization layer and COTS platform
F1
O-DU: RLC/MAC/PHY-high
Open Front Haul
O-RU: PHY-low/RF
Source: O-RAN Alliance
CP: Control Plane
MAC: Media Access Control
MANO: Management and Orchestration
NFVI: Network Functions Virtualisation Infrastructure
ONAP: Open Network Automation Platform
PDCP: Packet Data Convergence Protocol
PHY: PHYsical layer
RAT: Radio Access Technology
RF: Radio Frequency
RLC: Radio Link Control
RRC: Radio Resource Control
SDAP: Service Data Adaptation Protocol
UP: User Data Plane

Source: O-RAN Alliance, 2019

A recent important step in the development of the Open RAN ecosystem was an alliance agreement between the two organizations to ensure they were in alignment in developing interoperable, disaggregated and Open RAN solutions. The new agreement allows the two groups to share information, reference specifications and conduct joint testing and integration efforts.

Inherent in Open RAN is support for existing radio access networks in addition to 5G Nonstandalone (NSA) and Standalone (SA) networks. There are many parts of the world where all of these various technology generations must be supported; Open RAN actually allows that to happen on the same infrastructure.

To achieve this goal, the Open RAN movement helps enable a broader and vibrant open ecosystem of complete solutions and solution components that take advantage of the latest capabilities of GPPs, both at a software level and also using readily available programmable offload mechanisms such as field-programmable gate arrays (FPGA), and open interfaces.

Virtualization and openness

It is important to understand that virtualization and openness are not the same thing. Virtualization is disaggregation of hardware and software by abstracting the software application from the underlying hardware. A RAN can be virtualized but not be open – i.e., the software and/or the hardware could be proprietary, or the interfaces could be closed.

Being truly “open” means that there are reference designs and standards for hardware and software such that there are open interfaces with no proprietary interfaces and/or hardware in the RAN. For example, a COTS remote radio head/unit (RRH/U) from Vendor A will be able to talk via open interfaces to (proprietary) software running on a COTS server with (virtualized) network functions from Vendor B.

Note that openness does not mean that all hardware and software will be the identical for all mobile networks. Vendors will compete to produce all of the hardware and software such that operators will have a broad selection in terms of scale, scope, features and cost. Due to the open interfaces and standardized hardware, the network software will run on COTS and talk to hardware and software from other vendors. This will lead to a wider procurement ecosystem from different vendors.

Open RAN components

The goal of this paper is not to describe in detail the technologies involved in Open RAN – the various technologies and architectures are complex and difficult to cover in a short white paper. There is a range of network architectures that are needed to address the specific needs of different mobile operators around the world and it is expected that vendors will interoperate to create customized solutions to meet these requirements.

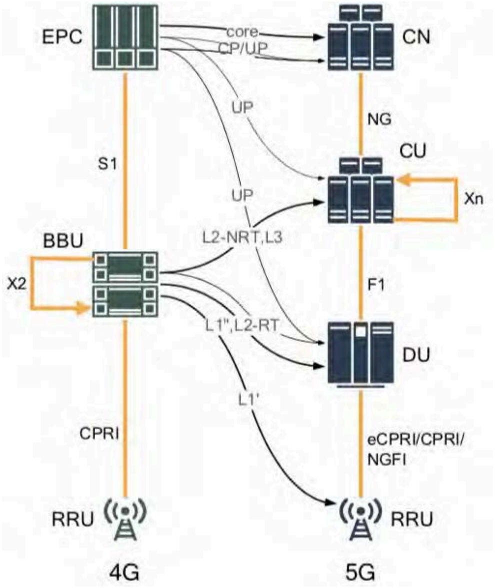
Moving forward into the world of 5G NR which, in 3GPP terms are Release 15 and beyond, the specifications require the RAN to become a new, disaggregated grouping of functional elements (as has been discussed earlier in this paper). The 5G base station, known as the gNB (as opposed to the eNodeB or eNB in LTE), is comprised of several functional units:

- The radio unit (RU) which comprises the RF chain, to transmit or receive the over-the-air signal and provide corresponding transformation of the analog radio signal and the digital signals.
- The distributed unit (DU) which handles the lower layers of the baseband processing up through the PDCP layer of the protocol stack. In legacy systems, this runs on a proprietary hardware appliance, but today's software (which runs on COTS) allows this function to be virtualized. Since it is virtualized, this gives flexibility in terms of placing the processes at different locations which may include the cell site, far edge locations and/or the centralized locations. These functional splits are defined in the 3GPP specifications and their placement is selected based on type of transport available to the cell sites.
- The centralized unit (CU) handles all higher layer functions of the protocol stack from PDCP and above.

As has been stated, the goal of Open RAN is to create open interfaces so that the hardware and software from different vendors can interoperate and talk to each other. One key initiative is the TIP Evenstar program which has developed a Remote Radio Head (RRH) that will be available in the second half of 2020. The Evenstar RRH decouples the base components of the RRH and will support the O-RAN Central Unit-Distributed Unit (CU-DU) architectural split known as 7.2. Beyond this, other vendors including MTI, Gigatera Communications, NEC, Airspan and Fujitsu have announced that they plan to provide radios in various configurations which will adhere to Open RAN specifications.

The following graphic shows the 4G RAN and core network as compared to the 5G RAN and core.

Figure 3: 4G RAN and the CU-DU Split in the 5G RAN



Source: Transport network support of IMT-2020/5G, ITU-T Report, February 2018

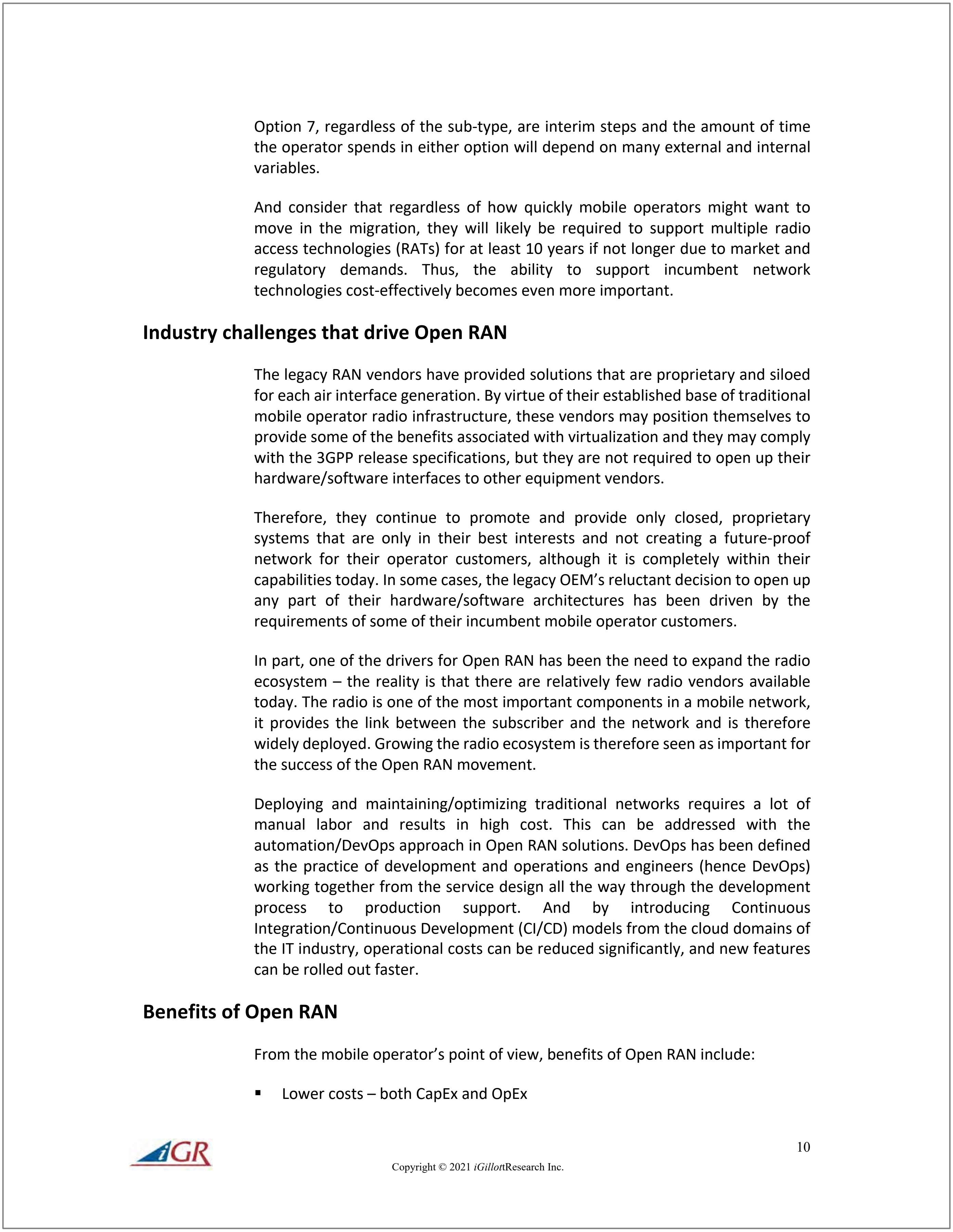
Note that in 5G, the BBU function from LTE is split between the CU and DU and this depends on which path the mobile operator is taking toward 5G, as there are many options that accommodate incumbent 2G, 3G and 4G networks, as well as the level of integration between the current network and a new 5G network.

The 3GPP defined multiple deployment options for carriers that are migrating to 5G NR from LTE. Two of the most likely paths are:

- **Option 1 to Option 3x to Option 7x to Option 4a to Option 2:** This path assumed that the operator already has an extensive RAN and a core network (EPC) that it wants to leverage before introducing a 5G core. The current roadmap assumes that Option 3 is already deployed, that Option 2 will be deployed when ready, and that the two configurations will coexist for some time. This path involves using multiple radio access technologies.

- **Option 1 to Option 3x to Option 4a to Option 2:** This path also assumes the existence of a RAN and core, but the move directly to 4a implies that 5G RAN coverage gets built out, the 5G core introduced and then the operator moves directly to 4a or Option 2.

It is *iG*R's understanding that the main differences between these two routes involve the extent of the changes and how long the process takes. These options enable operators to leverage the existing EPC that they have in their networks and allow for a migration path towards 5GC. It appears that both Option 3 and



Option 7, regardless of the sub-type, are interim steps and the amount of time the operator spends in either option will depend on many external and internal variables.

And consider that regardless of how quickly mobile operators might want to move in the migration, they will likely be required to support multiple radio access technologies (RATs) for at least 10 years if not longer due to market and regulatory demands. Thus, the ability to support incumbent network technologies cost-effectively becomes even more important.

Industry challenges that drive Open RAN

The legacy RAN vendors have provided solutions that are proprietary and siloed for each air interface generation. By virtue of their established base of traditional mobile operator radio infrastructure, these vendors may position themselves to provide some of the benefits associated with virtualization and they may comply with the 3GPP release specifications, but they are not required to open up their hardware/software interfaces to other equipment vendors.

Therefore, they continue to promote and provide only closed, proprietary systems that are only in their best interests and not creating a future-proof network for their operator customers, although it is completely within their capabilities today. In some cases, the legacy OEM’s reluctant decision to open up any part of their hardware/software architectures has been driven by the requirements of some of their incumbent mobile operator customers.

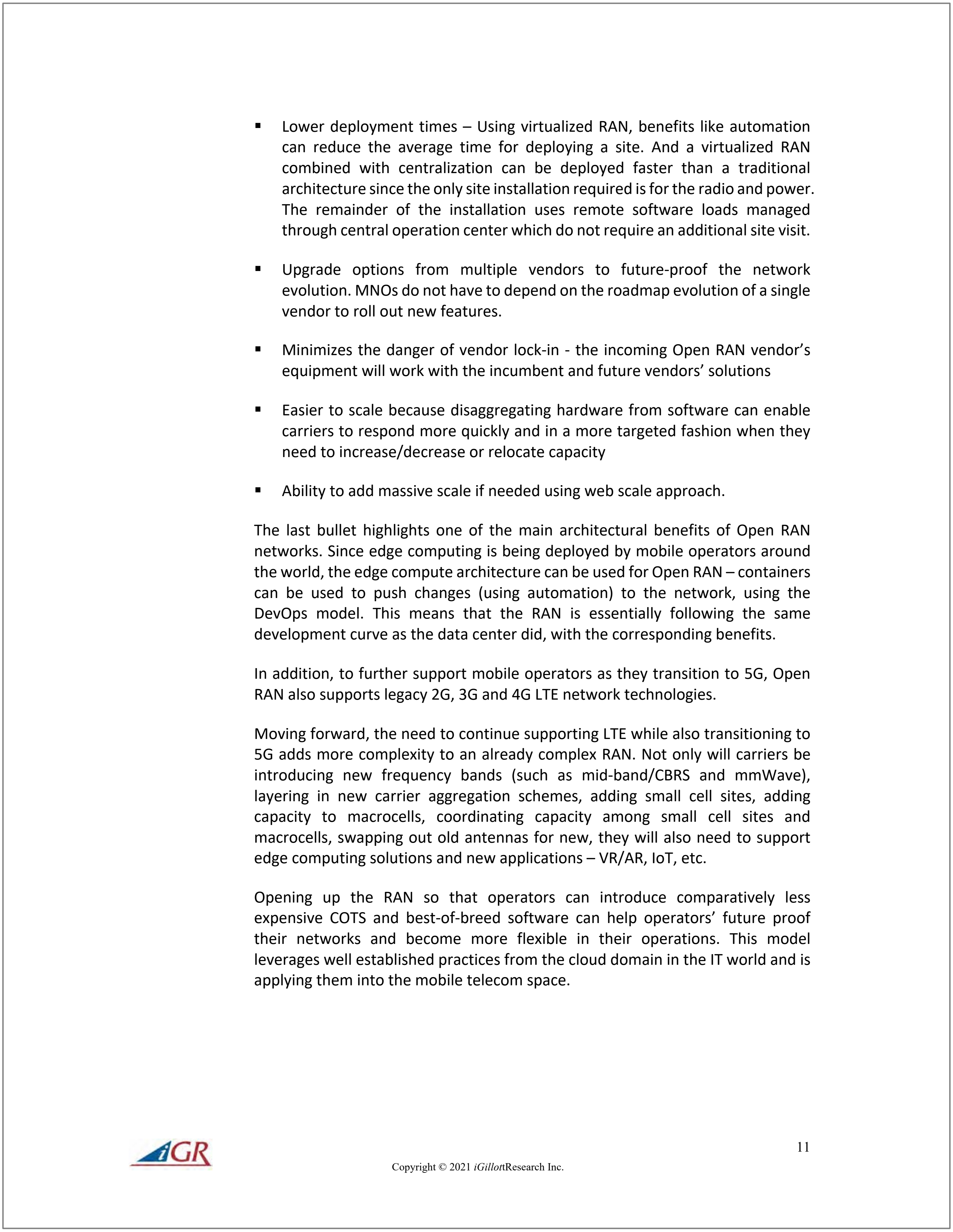
In part, one of the drivers for Open RAN has been the need to expand the radio ecosystem – the reality is that there are relatively few radio vendors available today. The radio is one of the most important components in a mobile network, it provides the link between the subscriber and the network and is therefore widely deployed. Growing the radio ecosystem is therefore seen as important for the success of the Open RAN movement.

Deploying and maintaining/optimizing traditional networks requires a lot of manual labor and results in high cost. This can be addressed with the automation/DevOps approach in Open RAN solutions. DevOps has been defined as the practice of development and operations and engineers (hence DevOps) working together from the service design all the way through the development process to production support. And by introducing Continuous Integration/Continuous Development (CI/CD) models from the cloud domains of the IT industry, operational costs can be reduced significantly, and new features can be rolled out faster.

Benefits of Open RAN

From the mobile operator’s point of view, benefits of Open RAN include:

- Lower costs – both CapEx and OpEx



- Lower deployment times – Using virtualized RAN, benefits like automation can reduce the average time for deploying a site. And a virtualized RAN combined with centralization can be deployed faster than a traditional architecture since the only site installation required is for the radio and power. The remainder of the installation uses remote software loads managed through central operation center which do not require an additional site visit.

- Upgrade options from multiple vendors to future-proof the network evolution. MNOs do not have to depend on the roadmap evolution of a single vendor to roll out new features.

- Minimizes the danger of vendor lock-in - the incoming Open RAN vendor's equipment will work with the incumbent and future vendors' solutions

- Easier to scale because disaggregating hardware from software can enable carriers to respond more quickly and in a more targeted fashion when they need to increase/decrease or relocate capacity

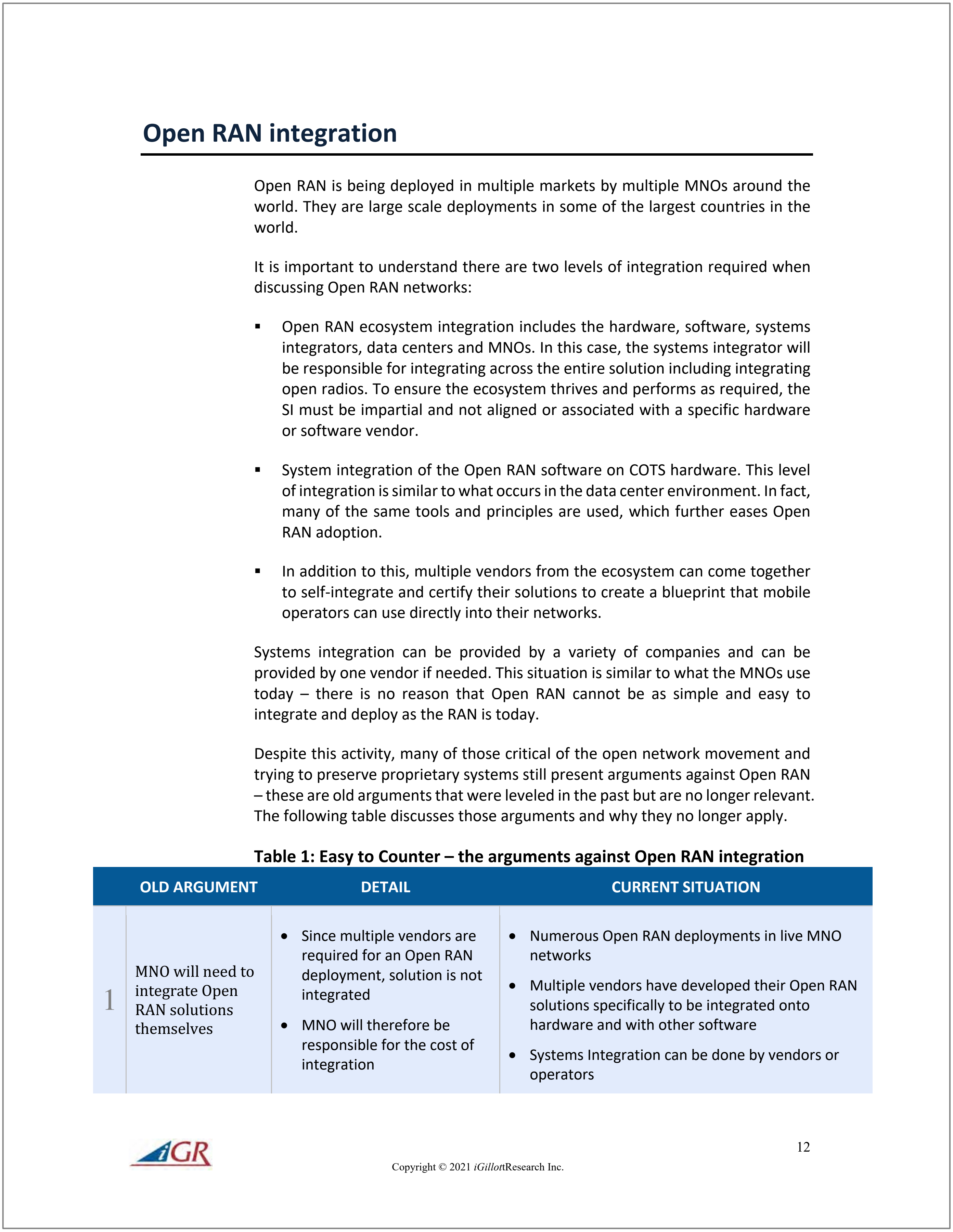
- Ability to add massive scale if needed using web scale approach.

The last bullet highlights one of the main architectural benefits of Open RAN networks. Since edge computing is being deployed by mobile operators around the world, the edge compute architecture can be used for Open RAN – containers can be used to push changes (using automation) to the network, using the DevOps model. This means that the RAN is essentially following the same development curve as the data center did, with the corresponding benefits.

In addition, to further support mobile operators as they transition to 5G, Open RAN also supports legacy 2G, 3G and 4G LTE network technologies.

Moving forward, the need to continue supporting LTE while also transitioning to 5G adds more complexity to an already complex RAN. Not only will carriers be introducing new frequency bands (such as mid-band/CBRS and mmWave), layering in new carrier aggregation schemes, adding small cell sites, adding capacity to macrocells, coordinating capacity among small cell sites and macrocells, swapping out old antennas for new, they will also need to support edge computing solutions and new applications – VR/AR, IoT, etc.

Opening up the RAN so that operators can introduce comparatively less expensive COTS and best-of-breed software can help operators' future proof their networks and become more flexible in their operations. This model leverages well established practices from the cloud domain in the IT world and is applying them into the mobile telecom space.



Open RAN integration

Open RAN is being deployed in multiple markets by multiple MNOs around the world. They are large scale deployments in some of the largest countries in the world.

It is important to understand there are two levels of integration required when discussing Open RAN networks:

- Open RAN ecosystem integration includes the hardware, software, systems integrators, data centers and MNOs. In this case, the systems integrator will be responsible for integrating across the entire solution including integrating open radios. To ensure the ecosystem thrives and performs as required, the SI must be impartial and not aligned or associated with a specific hardware or software vendor.

- System integration of the Open RAN software on COTS hardware. This level of integration is similar to what occurs in the data center environment. In fact, many of the same tools and principles are used, which further eases Open RAN adoption.

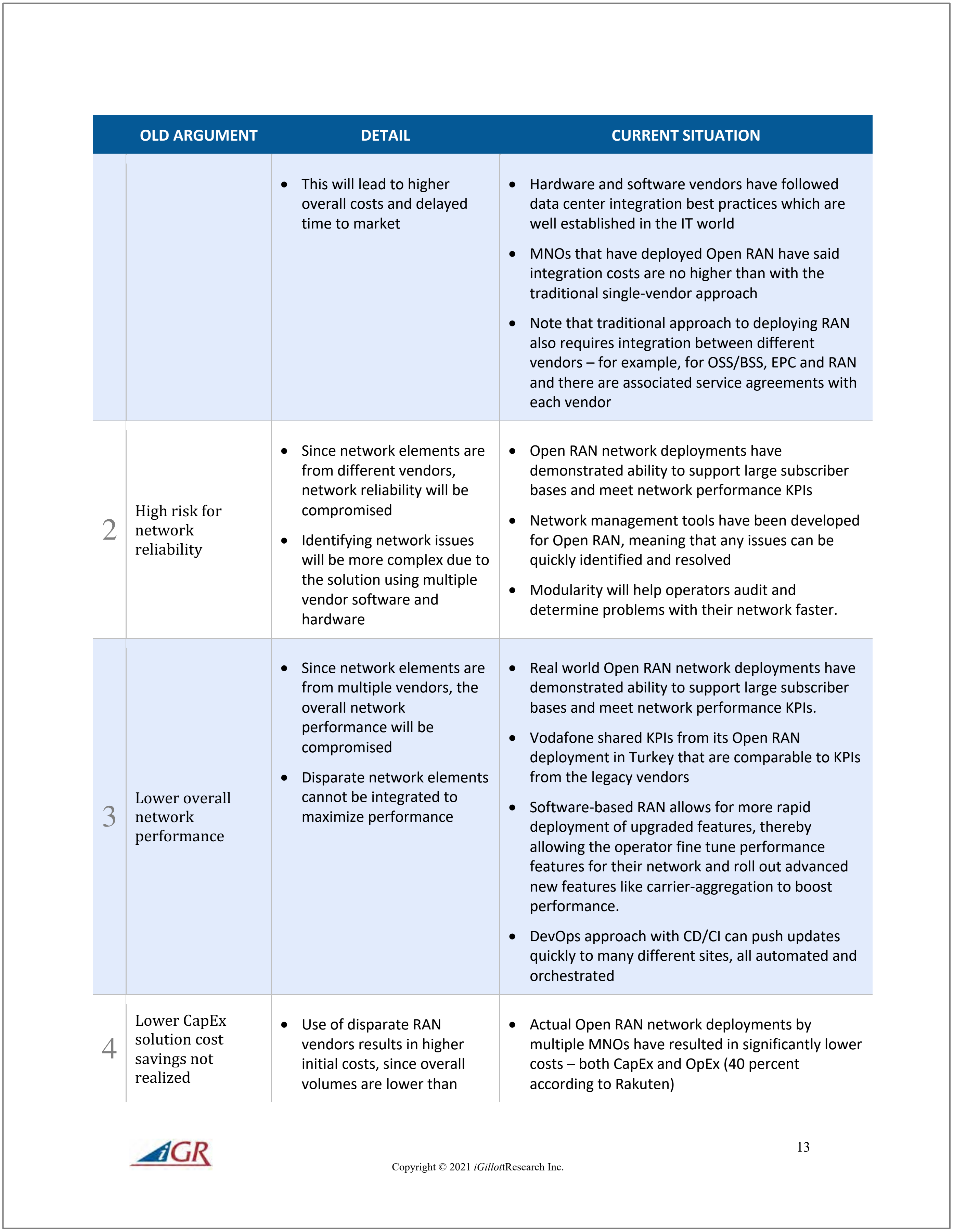
- In addition to this, multiple vendors from the ecosystem can come together to self-integrate and certify their solutions to create a blueprint that mobile operators can use directly into their networks.

Systems integration can be provided by a variety of companies and can be provided by one vendor if needed. This situation is similar to what the MNOs use today – there is no reason that Open RAN cannot be as simple and easy to integrate and deploy as the RAN is today.

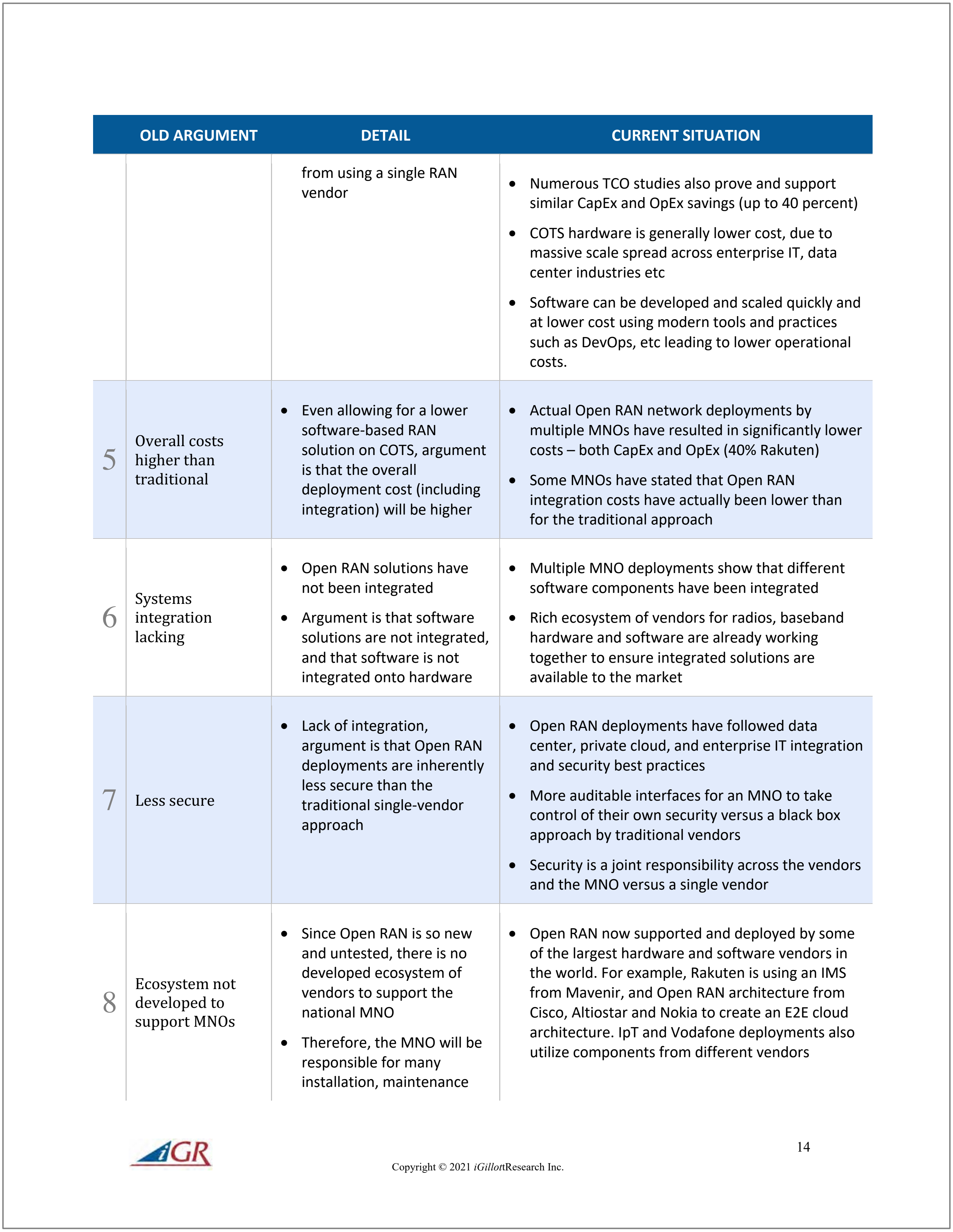
Despite this activity, many of those critical of the open network movement and trying to preserve proprietary systems still present arguments against Open RAN – these are old arguments that were leveled in the past but are no longer relevant. The following table discusses those arguments and why they no longer apply.

Table 1: Easy to Counter – the arguments against Open RAN integration

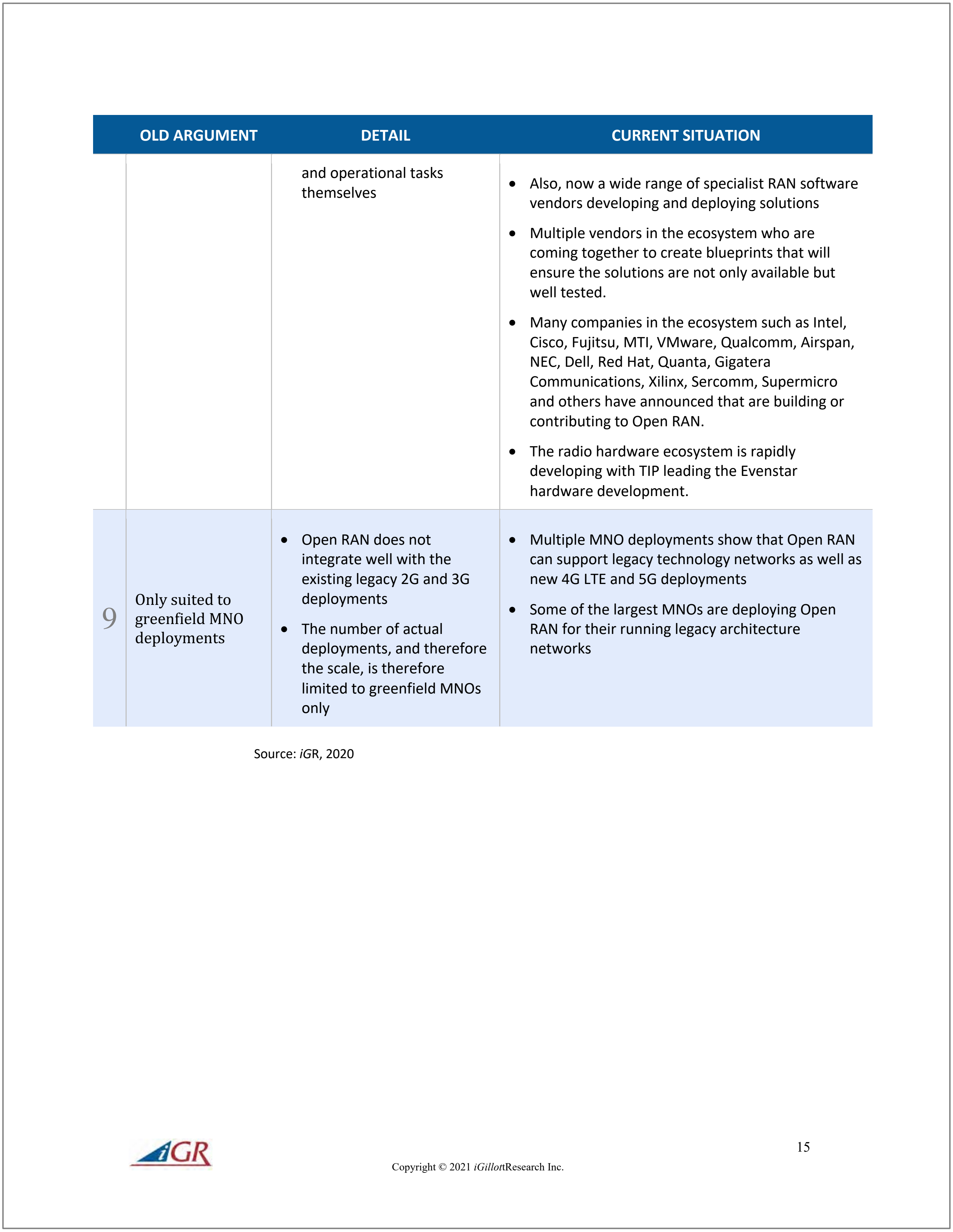
OLD ARGUMENT		DETAIL	CURRENT SITUATION
1	MNO will need to integrate Open RAN solutions themselves	• Since multiple vendors are required for an Open RAN deployment, solution is not integrated • MNO will therefore be responsible for the cost of integration	• Numerous Open RAN deployments in live MNO networks • Multiple vendors have developed their Open RAN solutions specifically to be integrated onto hardware and with other software • Systems Integration can be done by vendors or operators



OLD ARGUMENT		DETAIL	CURRENT SITUATION
		• This will lead to higher overall costs and delayed time to market	• Hardware and software vendors have followed data center integration best practices which are well established in the IT world • MNOs that have deployed Open RAN have said integration costs are no higher than with the traditional single-vendor approach • Note that traditional approach to deploying RAN also requires integration between different vendors – for example, for OSS/BSS, EPC and RAN and there are associated service agreements with each vendor
2	High risk for network reliability	• Since network elements are from different vendors, network reliability will be compromised • Identifying network issues will be more complex due to the solution using multiple vendor software and hardware	• Open RAN network deployments have demonstrated ability to support large subscriber bases and meet network performance KPIs • Network management tools have been developed for Open RAN, meaning that any issues can be quickly identified and resolved • Modularity will help operators audit and determine problems with their network faster.
3	Lower overall network performance	• Since network elements are from multiple vendors, the overall network performance will be compromised • Disparate network elements cannot be integrated to maximize performance	• Real world Open RAN network deployments have demonstrated ability to support large subscriber bases and meet network performance KPIs. • Vodafone shared KPIs from its Open RAN deployment in Turkey that are comparable to KPIs from the legacy vendors • Software-based RAN allows for more rapid deployment of upgraded features, thereby allowing the operator fine tune performance features for their network and roll out advanced new features like carrier-aggregation to boost performance. • DevOps approach with CD/CI can push updates quickly to many different sites, all automated and orchestrated
4	Lower CapEx solution cost savings not realized	• Use of disparate RAN vendors results in higher initial costs, since overall volumes are lower than	• Actual Open RAN network deployments by multiple MNOs have resulted in significantly lower costs – both CapEx and OpEx (40 percent according to Rakuten)

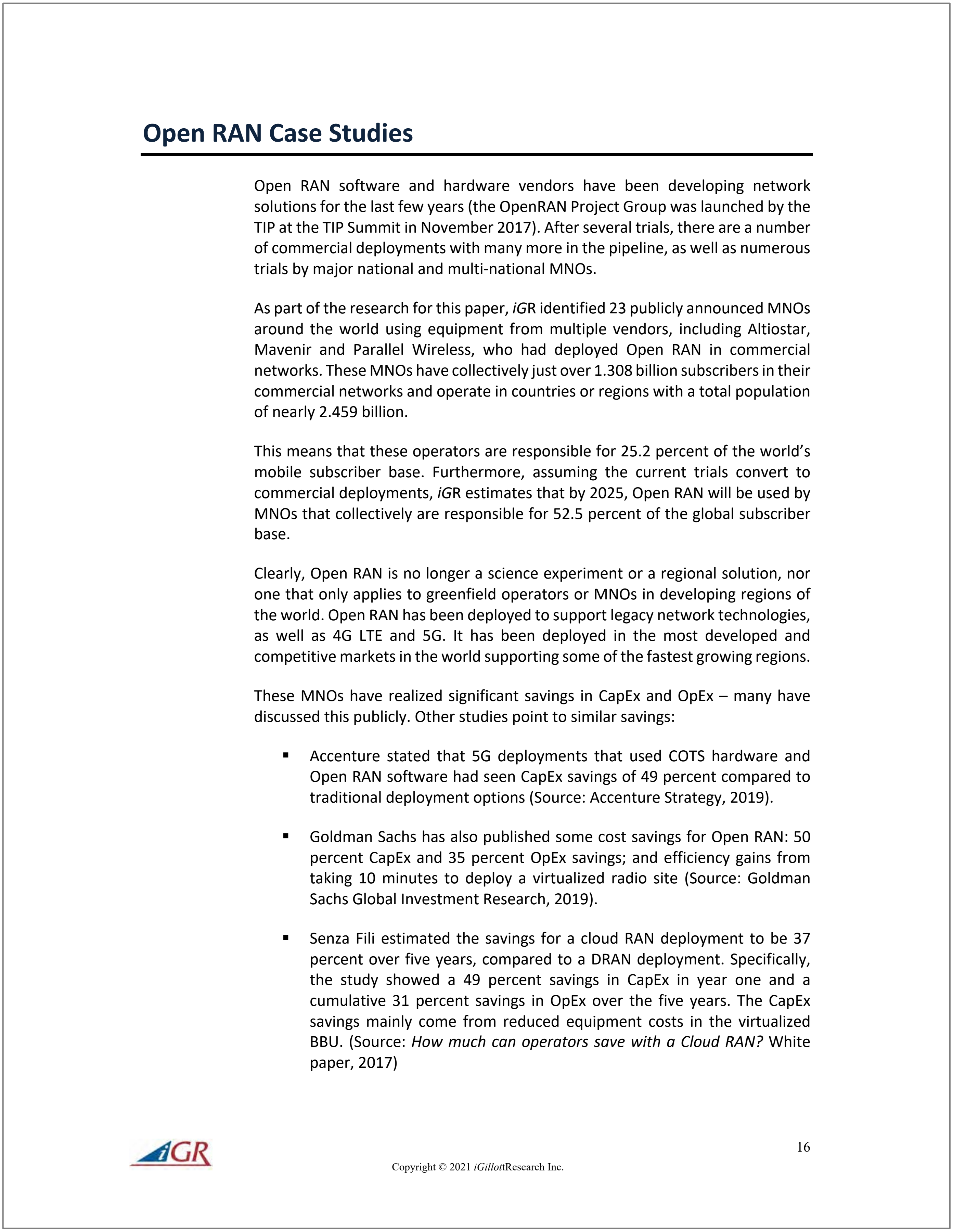


OLD ARGUMENT		DETAIL	CURRENT SITUATION
		from using a single RAN vendor	• Numerous TCO studies also prove and support similar CapEx and OpEx savings (up to 40 percent) • COTS hardware is generally lower cost, due to massive scale spread across enterprise IT, data center industries etc • Software can be developed and scaled quickly and at lower cost using modern tools and practices such as DevOps, etc leading to lower operational costs.
5	Overall costs higher than traditional	• Even allowing for a lower software-based RAN solution on COTS, argument is that the overall deployment cost (including integration) will be higher	• Actual Open RAN network deployments by multiple MNOs have resulted in significantly lower costs – both CapEx and OpEx (40% Rakuten) • Some MNOs have stated that Open RAN integration costs have actually been lower than for the traditional approach
6	Systems integration lacking	• Open RAN solutions have not been integrated • Argument is that software solutions are not integrated, and that software is not integrated onto hardware	• Multiple MNO deployments show that different software components have been integrated • Rich ecosystem of vendors for radios, baseband hardware and software are already working together to ensure integrated solutions are available to the market
7	Less secure	• Lack of integration, argument is that Open RAN deployments are inherently less secure than the traditional single-vendor approach	• Open RAN deployments have followed data center, private cloud, and enterprise IT integration and security best practices • More auditable interfaces for an MNO to take control of their own security versus a black box approach by traditional vendors • Security is a joint responsibility across the vendors and the MNO versus a single vendor
8	Ecosystem not developed to support MNOs	• Since Open RAN is so new and untested, there is no developed ecosystem of vendors to support the national MNO • Therefore, the MNO will be responsible for many installation, maintenance	• Open RAN now supported and deployed by some of the largest hardware and software vendors in the world. For example, Rakuten is using an IMS from Mavenir, and Open RAN architecture from Cisco, Altiostar and Nokia to create an E2E cloud architecture. IpT and Vodafone deployments also utilize components from different vendors



	OLD ARGUMENT	DETAIL	CURRENT SITUATION
		and operational tasks themselves	• Also, now a wide range of specialist RAN software vendors developing and deploying solutions • Multiple vendors in the ecosystem who are coming together to create blueprints that will ensure the solutions are not only available but well tested. • Many companies in the ecosystem such as Intel, Cisco, Fujitsu, MTI, VMware, Qualcomm, Airspan, NEC, Dell, Red Hat, Quanta, Gigatera Communications, Xilinx, Sercomm, Supermicro and others have announced that are building or contributing to Open RAN. • The radio hardware ecosystem is rapidly developing with TIP leading the Evenstar hardware development.
9	Only suited to greenfield MNO deployments	• Open RAN does not integrate well with the existing legacy 2G and 3G deployments • The number of actual deployments, and therefore the scale, is therefore limited to greenfield MNOs only	• Multiple MNO deployments show that Open RAN can support legacy technology networks as well as new 4G LTE and 5G deployments • Some of the largest MNOs are deploying Open RAN for their running legacy architecture networks

Source: *i*GR, 2020



Open RAN Case Studies

Open RAN software and hardware vendors have been developing network solutions for the last few years (the OpenRAN Project Group was launched by the TIP at the TIP Summit in November 2017). After several trials, there are a number of commercial deployments with many more in the pipeline, as well as numerous trials by major national and multi-national MNOs.

As part of the research for this paper, *iG*R identified 23 publicly announced MNOs around the world using equipment from multiple vendors, including Altiostar, Mavenir and Parallel Wireless, who had deployed Open RAN in commercial networks. These MNOs have collectively just over 1.308 billion subscribers in their commercial networks and operate in countries or regions with a total population of nearly 2.459 billion.

This means that these operators are responsible for 25.2 percent of the world's mobile subscriber base. Furthermore, assuming the current trials convert to commercial deployments, *iG*R estimates that by 2025, Open RAN will be used by MNOs that collectively are responsible for 52.5 percent of the global subscriber base.

Clearly, Open RAN is no longer a science experiment or a regional solution, nor one that only applies to greenfield operators or MNOs in developing regions of the world. Open RAN has been deployed to support legacy network technologies, as well as 4G LTE and 5G. It has been deployed in the most developed and competitive markets in the world supporting some of the fastest growing regions.

These MNOs have realized significant savings in CapEx and OpEx – many have discussed this publicly. Other studies point to similar savings:

- Accenture stated that 5G deployments that used COTS hardware and Open RAN software had seen CapEx savings of 49 percent compared to traditional deployment options (Source: Accenture Strategy, 2019).
- Goldman Sachs has also published some cost savings for Open RAN: 50 percent CapEx and 35 percent OpEx savings; and efficiency gains from taking 10 minutes to deploy a virtualized radio site (Source: Goldman Sachs Global Investment Research, 2019).
- Senza Fili estimated the savings for a cloud RAN deployment to be 37 percent over five years, compared to a DRAN deployment. Specifically, the study showed a 49 percent savings in CapEx in year one and a cumulative 31 percent savings in OpEx over the five years. The CapEx savings mainly come from reduced equipment costs in the virtualized BBU. (Source: *How much can operators save with a Cloud RAN?* White paper, 2017)

- Strategy Analytics modelled the TCO of Open RAN over a five-year period. This model showed 40 percent lower CapEx and 34 percent lower OpEx compared to a legacy RAN. Strategy Analytics stated Open RAN cost savings of $93.852 per macrocell site excluding cell site costs and $204,390 per macrocell site including cell site costs. (Source: Strategy Analytics, 2019).

This section details some of the major Open RAN deployments around the world.

Dish Network

DISH Network, through its subsidiaries, the company provides television entertainment to over eleven million customers with its satellite DISH TV and streaming SLING TV services. In 2020, the company became a nationwide U.S. wireless carrier through the acquisition of Boost Mobile.

DISH has invested over $20 billion in wireless spectrum assets to date to enter the wireless industry and is currently building the United States' first cloud-native, Open RAN-based 5G broadband network. The company has participated in every FCC spectrum auction since 2008 - its spectrum acquisitions include: the FCC's 2008 700 MHz auction; a 2011 acquisition of two satellite service companies with AWS-4 spectrum holdings; the FCC's 2014 H Block auction; the FCC's 2017 600 MHz Incentive auction; the FCC's 2019 24/28 GHz auctions; and the FCC's 2020 Citizens Broadband Radio Service (CBRS) auction.

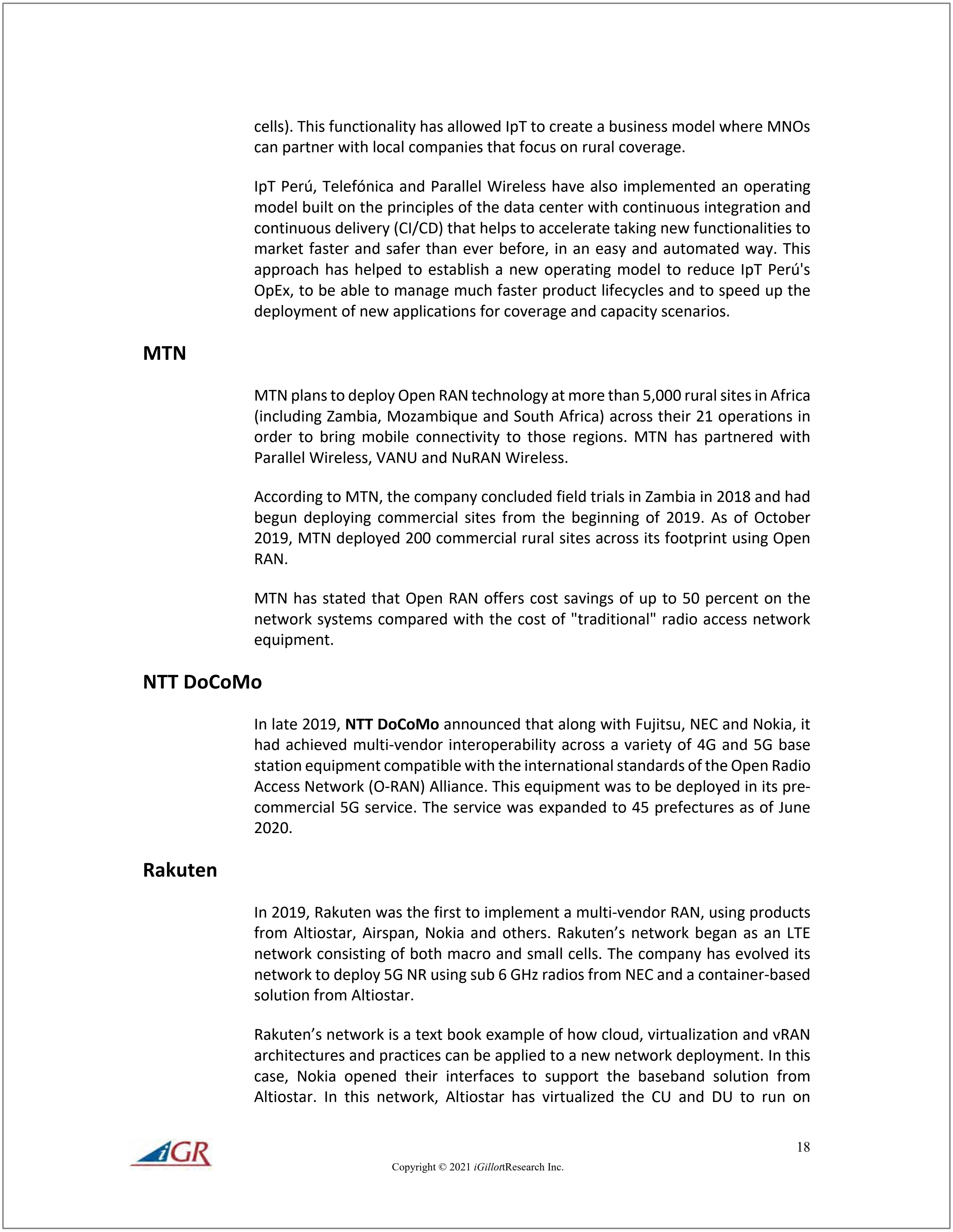
Utilizing Open RAN cloud-native wireless architecture, DISH plans to use its spectrum to deploy the nation's first virtualized, standalone 5G broadband network. DISH recently launched its first Open RAN 5G radio and antenna trial cell site in Littleton, Colorado. DISH is expecting to cover 20 percent of the U.S. population by June 2022 and 70 percent by June 2023.

To date, Dish has announced several vendors for its Open RAN network, including Mavenir, Altiostar, MTI, Qualcomm, Intel, and Fujitsu.

IpT

Internet para Todos Perú (IpT Peru) launched in May 2019. The company is owned by Telefónica, Facebook, IDB Invest and CAF banks. IpT Peru has deployed hundreds of new mobile sites in Peru using the Parallel Wireless virtualized and automated Open RAN architecture.

With the Parallel Wireless OpenRAN Controller, IpT has created a multi-vendor, multi-operator, open ecosystem of interoperable components for the various RAN elements and from different vendors. All new radio units are self-configured by the software, which reduces the need for manual intervention. The self-optimization capability automates optimization across different RANs in IpT Peru's network, utilizing available RAN data from all RAN types (macros and small



cells). This functionality has allowed IpT to create a business model where MNOs can partner with local companies that focus on rural coverage.

IpT Perú, Telefónica and Parallel Wireless have also implemented an operating model built on the principles of the data center with continuous integration and continuous delivery (CI/CD) that helps to accelerate taking new functionalities to market faster and safer than ever before, in an easy and automated way. This approach has helped to establish a new operating model to reduce IpT Perú's OpEx, to be able to manage much faster product lifecycles and to speed up the deployment of new applications for coverage and capacity scenarios.

MTN

MTN plans to deploy Open RAN technology at more than 5,000 rural sites in Africa (including Zambia, Mozambique and South Africa) across their 21 operations in order to bring mobile connectivity to those regions. MTN has partnered with Parallel Wireless, VANU and NuRAN Wireless.

According to MTN, the company concluded field trials in Zambia in 2018 and had begun deploying commercial sites from the beginning of 2019. As of October 2019, MTN deployed 200 commercial rural sites across its footprint using Open RAN.

MTN has stated that Open RAN offers cost savings of up to 50 percent on the network systems compared with the cost of "traditional" radio access network equipment.

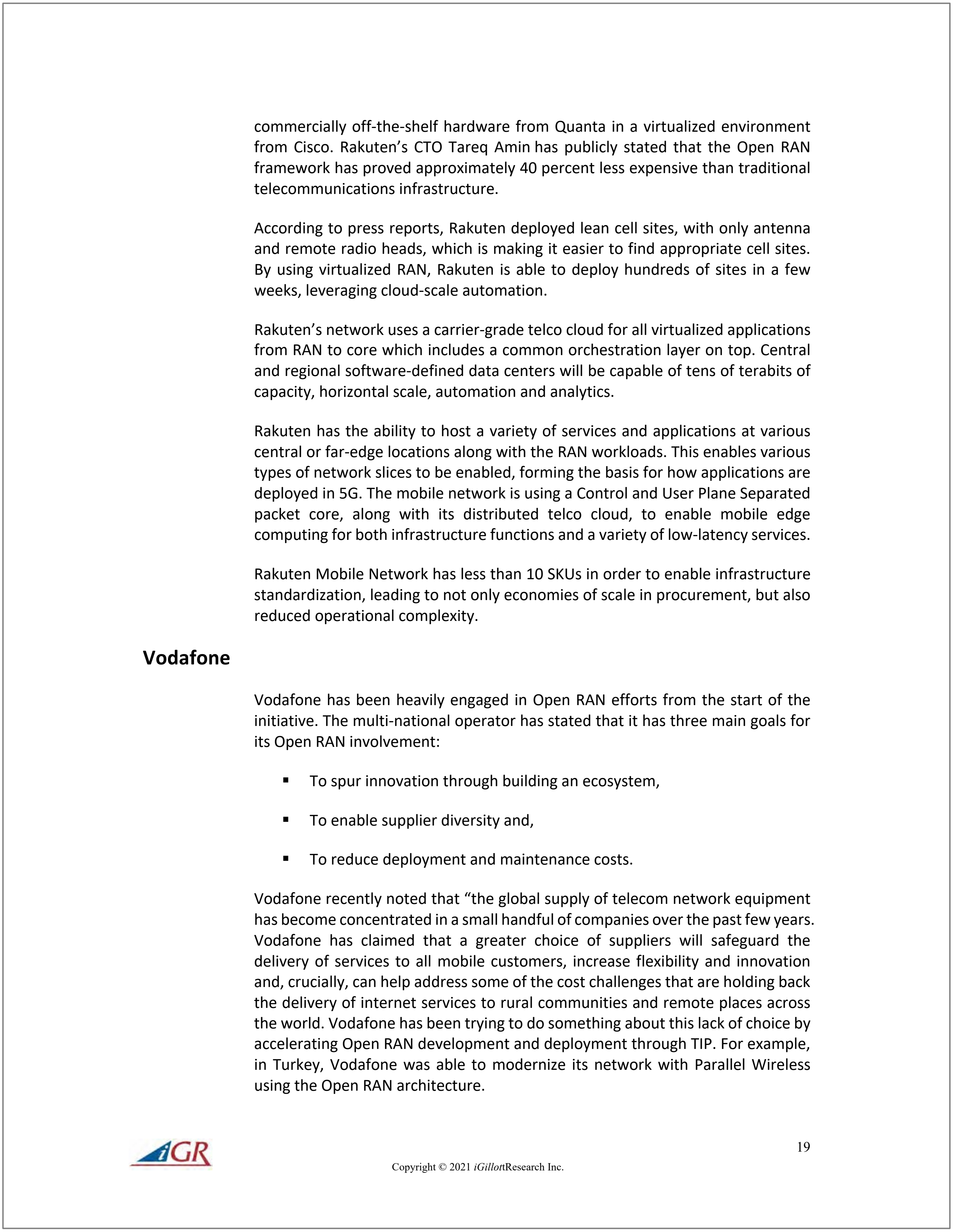
NTT DoCoMo

In late 2019, **NTT DoCoMo** announced that along with Fujitsu, NEC and Nokia, it had achieved multi-vendor interoperability across a variety of 4G and 5G base station equipment compatible with the international standards of the Open Radio Access Network (O-RAN) Alliance. This equipment was to be deployed in its pre-commercial 5G service. The service was expanded to 45 prefectures as of June 2020.

Rakuten

In 2019, Rakuten was the first to implement a multi-vendor RAN, using products from Altiostar, Airspan, Nokia and others. Rakuten’s network began as an LTE network consisting of both macro and small cells. The company has evolved its network to deploy 5G NR using sub 6 GHz radios from NEC and a container-based solution from Altiostar.

Rakuten’s network is a text book example of how cloud, virtualization and vRAN architectures and practices can be applied to a new network deployment. In this case, Nokia opened their interfaces to support the baseband solution from Altiostar. In this network, Altiostar has virtualized the CU and DU to run on



commercially off-the-shelf hardware from Quanta in a virtualized environment from Cisco. Rakuten’s CTO Tareq Amin has publicly stated that the Open RAN framework has proved approximately 40 percent less expensive than traditional telecommunications infrastructure.

According to press reports, Rakuten deployed lean cell sites, with only antenna and remote radio heads, which is making it easier to find appropriate cell sites. By using virtualized RAN, Rakuten is able to deploy hundreds of sites in a few weeks, leveraging cloud-scale automation.

Rakuten’s network uses a carrier-grade telco cloud for all virtualized applications from RAN to core which includes a common orchestration layer on top. Central and regional software-defined data centers will be capable of tens of terabits of capacity, horizontal scale, automation and analytics.

Rakuten has the ability to host a variety of services and applications at various central or far-edge locations along with the RAN workloads. This enables various types of network slices to be enabled, forming the basis for how applications are deployed in 5G. The mobile network is using a Control and User Plane Separated packet core, along with its distributed telco cloud, to enable mobile edge computing for both infrastructure functions and a variety of low-latency services.

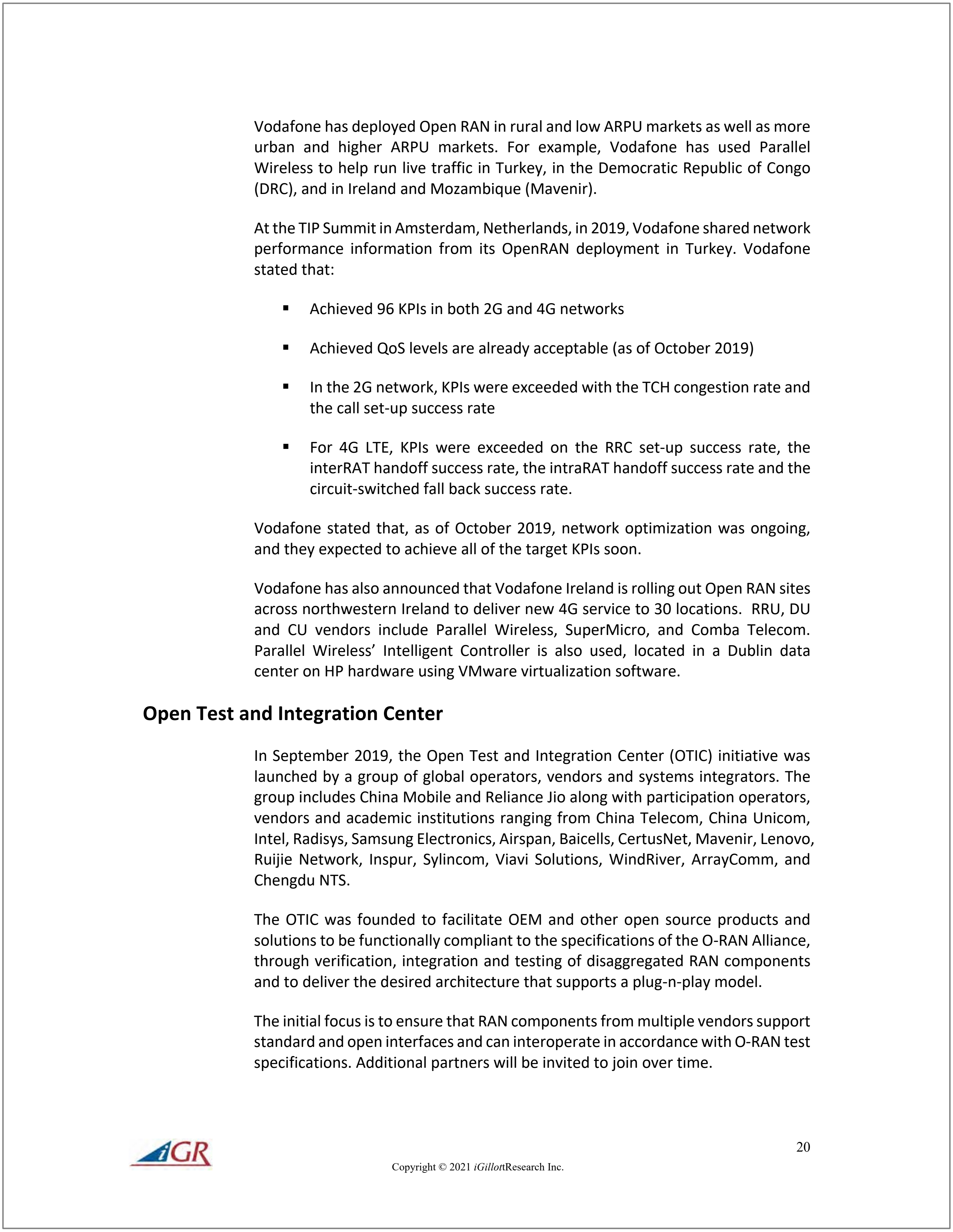
Rakuten Mobile Network has less than 10 SKUs in order to enable infrastructure standardization, leading to not only economies of scale in procurement, but also reduced operational complexity.

Vodafone

Vodafone has been heavily engaged in Open RAN efforts from the start of the initiative. The multi-national operator has stated that it has three main goals for its Open RAN involvement:

- To spur innovation through building an ecosystem,
- To enable supplier diversity and,
- To reduce deployment and maintenance costs.

Vodafone recently noted that “the global supply of telecom network equipment has become concentrated in a small handful of companies over the past few years. Vodafone has claimed that a greater choice of suppliers will safeguard the delivery of services to all mobile customers, increase flexibility and innovation and, crucially, can help address some of the cost challenges that are holding back the delivery of internet services to rural communities and remote places across the world. Vodafone has been trying to do something about this lack of choice by accelerating Open RAN development and deployment through TIP. For example, in Turkey, Vodafone was able to modernize its network with Parallel Wireless using the Open RAN architecture.



Vodafone has deployed Open RAN in rural and low ARPU markets as well as more urban and higher ARPU markets. For example, Vodafone has used Parallel Wireless to help run live traffic in Turkey, in the Democratic Republic of Congo (DRC), and in Ireland and Mozambique (Mavenir).

At the TIP Summit in Amsterdam, Netherlands, in 2019, Vodafone shared network performance information from its OpenRAN deployment in Turkey. Vodafone stated that:

- Achieved 96 KPIs in both 2G and 4G networks
- Achieved QoS levels are already acceptable (as of October 2019)
- In the 2G network, KPIs were exceeded with the TCH congestion rate and the call set-up success rate
- For 4G LTE, KPIs were exceeded on the RRC set-up success rate, the interRAT handoff success rate, the intraRAT handoff success rate and the circuit-switched fall back success rate.

Vodafone stated that, as of October 2019, network optimization was ongoing, and they expected to achieve all of the target KPIs soon.

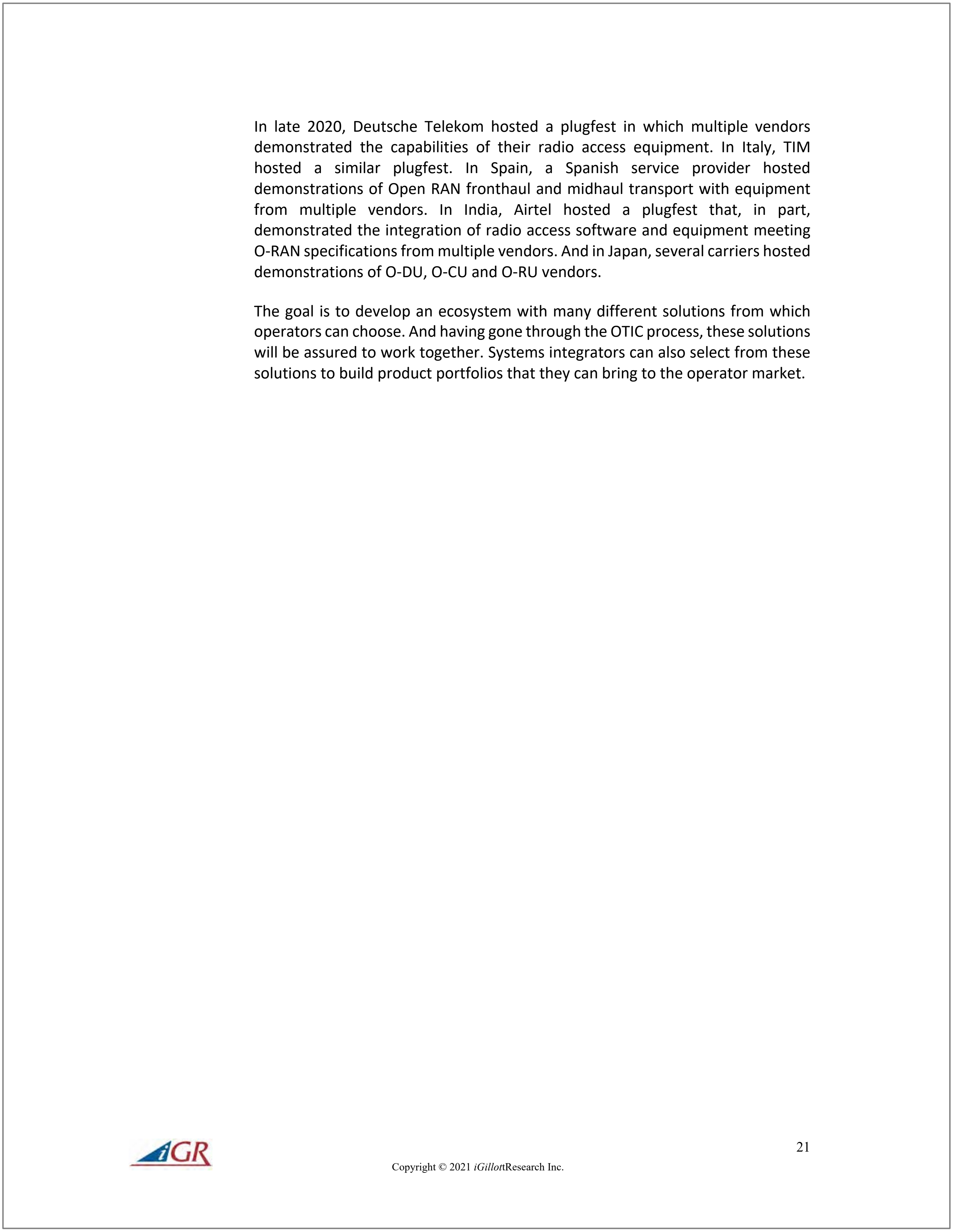
Vodafone has also announced that Vodafone Ireland is rolling out Open RAN sites across northwestern Ireland to deliver new 4G service to 30 locations. RRU, DU and CU vendors include Parallel Wireless, SuperMicro, and Comba Telecom. Parallel Wireless' Intelligent Controller is also used, located in a Dublin data center on HP hardware using VMware virtualization software.

Open Test and Integration Center

In September 2019, the Open Test and Integration Center (OTIC) initiative was launched by a group of global operators, vendors and systems integrators. The group includes China Mobile and Reliance Jio along with participation operators, vendors and academic institutions ranging from China Telecom, China Unicom, Intel, Radisys, Samsung Electronics, Airspan, Baicells, CertusNet, Mavenir, Lenovo, Ruijie Network, Inspur, Sylincom, Viavi Solutions, WindRiver, ArrayComm, and Chengdu NTS.

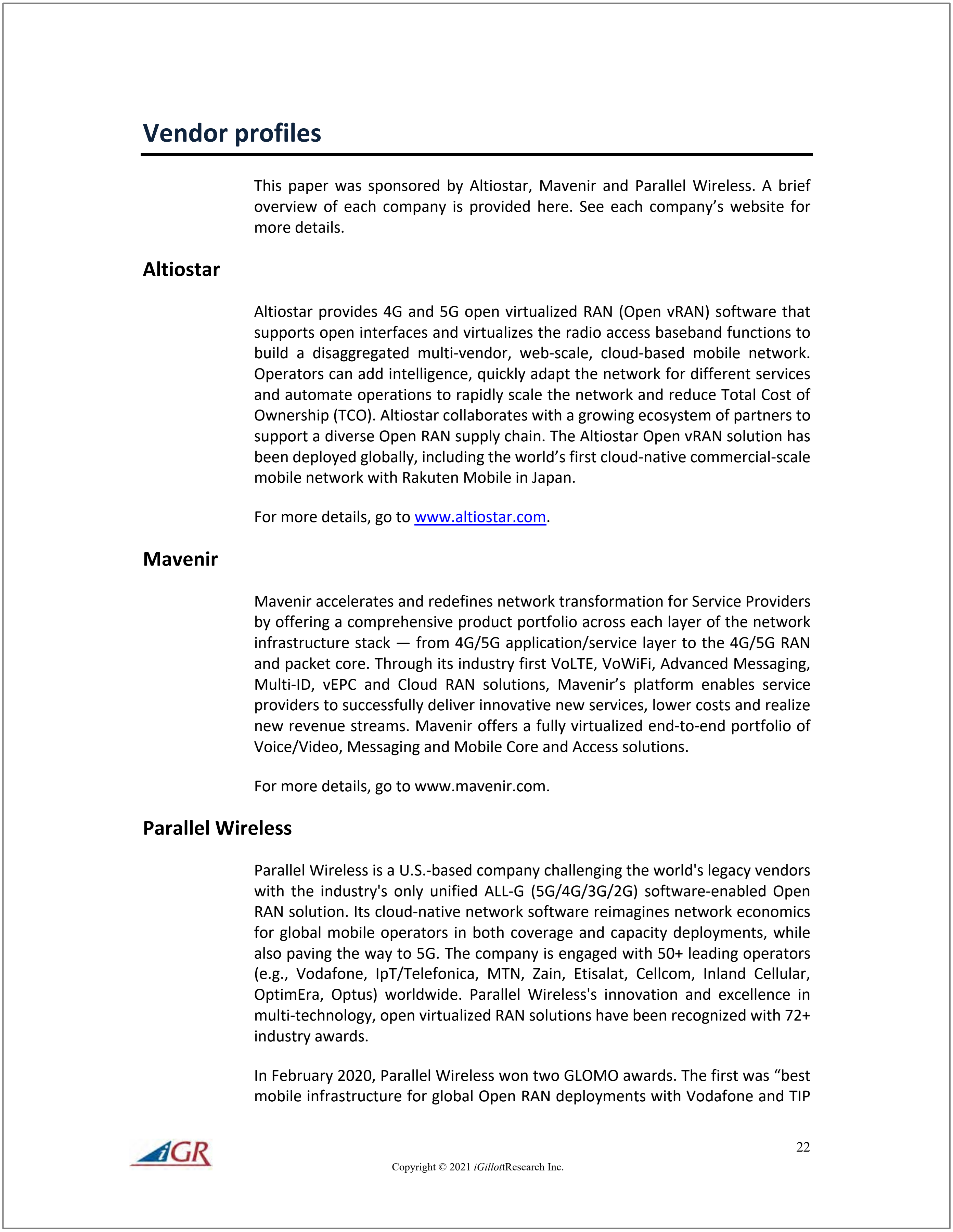
The OTIC was founded to facilitate OEM and other open source products and solutions to be functionally compliant to the specifications of the O-RAN Alliance, through verification, integration and testing of disaggregated RAN components and to deliver the desired architecture that supports a plug-n-play model.

The initial focus is to ensure that RAN components from multiple vendors support standard and open interfaces and can interoperate in accordance with O-RAN test specifications. Additional partners will be invited to join over time.



In late 2020, Deutsche Telekom hosted a plugfest in which multiple vendors demonstrated the capabilities of their radio access equipment. In Italy, TIM hosted a similar plugfest. In Spain, a Spanish service provider hosted demonstrations of Open RAN fronthaul and midhaul transport with equipment from multiple vendors. In India, Airtel hosted a plugfest that, in part, demonstrated the integration of radio access software and equipment meeting O-RAN specifications from multiple vendors. And in Japan, several carriers hosted demonstrations of O-DU, O-CU and O-RU vendors.

The goal is to develop an ecosystem with many different solutions from which operators can choose. And having gone through the OTIC process, these solutions will be assured to work together. Systems integrators can also select from these solutions to build product portfolios that they can bring to the operator market.



Vendor profiles

This paper was sponsored by Altiostar, Mavenir and Parallel Wireless. A brief overview of each company is provided here. See each company's website for more details.

Altiostar

Altiostar provides 4G and 5G open virtualized RAN (Open vRAN) software that supports open interfaces and virtualizes the radio access baseband functions to build a disaggregated multi-vendor, web-scale, cloud-based mobile network. Operators can add intelligence, quickly adapt the network for different services and automate operations to rapidly scale the network and reduce Total Cost of Ownership (TCO). Altiostar collaborates with a growing ecosystem of partners to support a diverse Open RAN supply chain. The Altiostar Open vRAN solution has been deployed globally, including the world's first cloud-native commercial-scale mobile network with Rakuten Mobile in Japan.

For more details, go to www.altiostar.com.

Mavenir

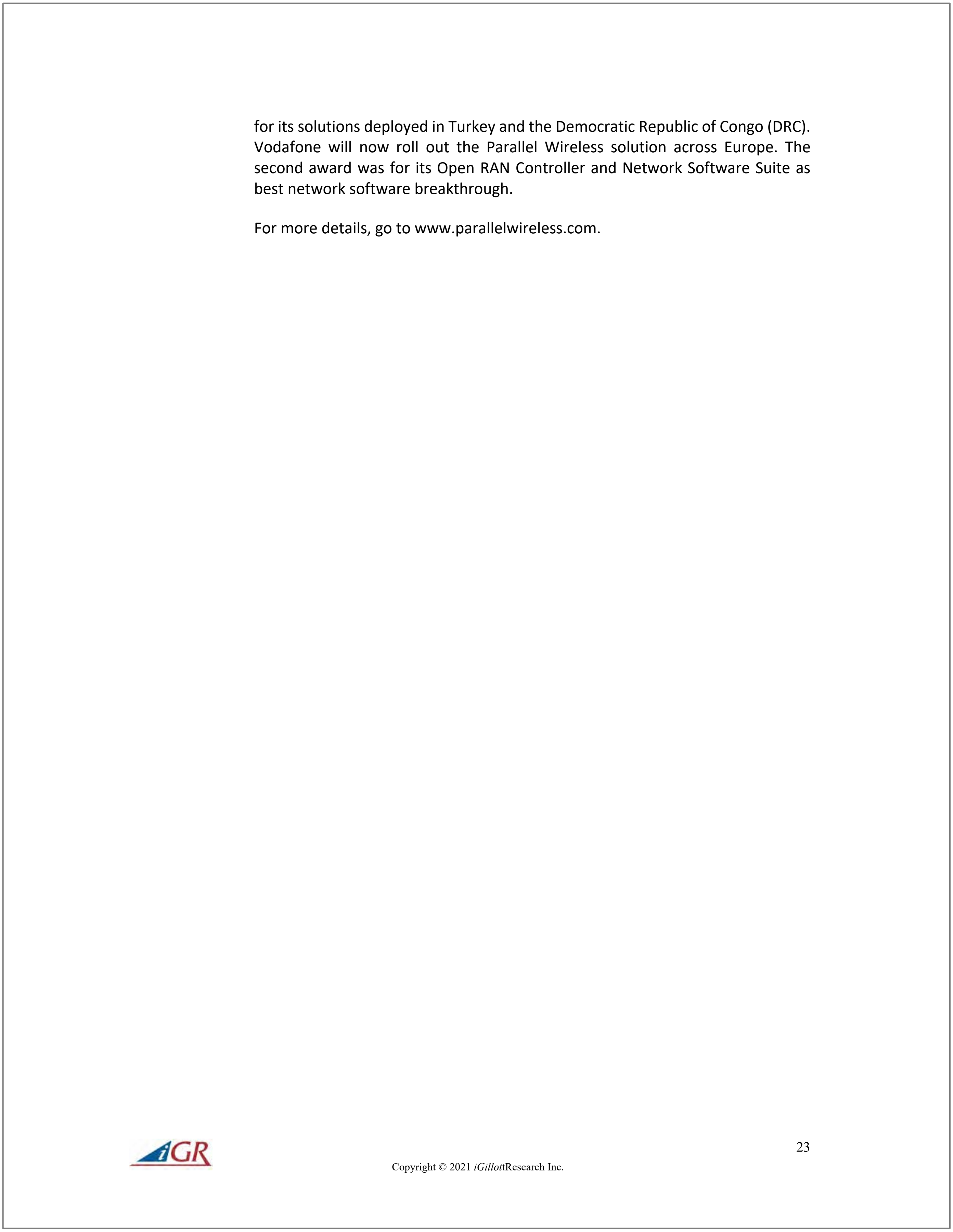
Mavenir accelerates and redefines network transformation for Service Providers by offering a comprehensive product portfolio across each layer of the network infrastructure stack — from 4G/5G application/service layer to the 4G/5G RAN and packet core. Through its industry first VoLTE, VoWiFi, Advanced Messaging, Multi-ID, vEPC and Cloud RAN solutions, Mavenir's platform enables service providers to successfully deliver innovative new services, lower costs and realize new revenue streams. Mavenir offers a fully virtualized end-to-end portfolio of Voice/Video, Messaging and Mobile Core and Access solutions.

For more details, go to www.mavenir.com.

Parallel Wireless

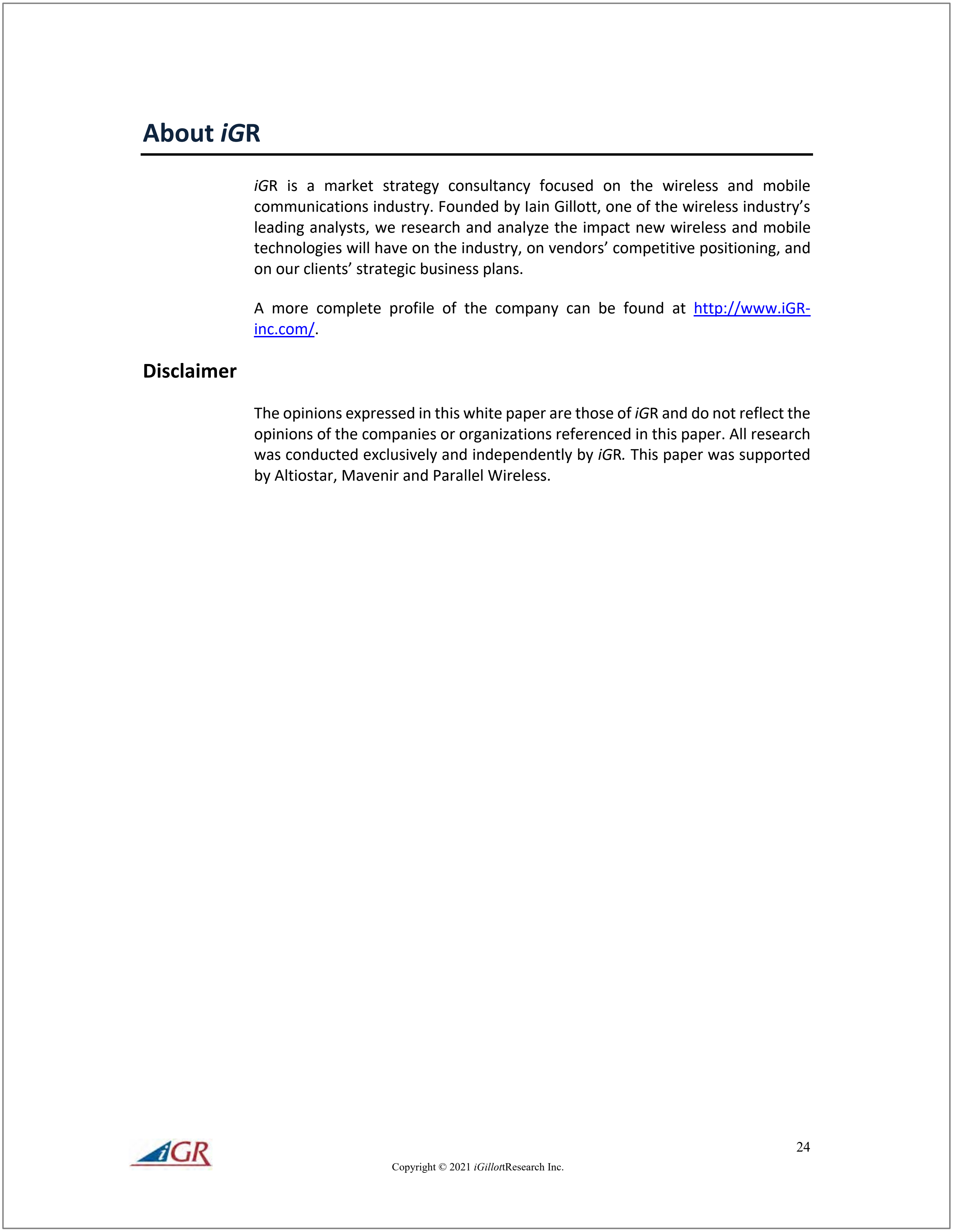
Parallel Wireless is a U.S.-based company challenging the world's legacy vendors with the industry's only unified ALL-G (5G/4G/3G/2G) software-enabled Open RAN solution. Its cloud-native network software reimagines network economics for global mobile operators in both coverage and capacity deployments, while also paving the way to 5G. The company is engaged with 50+ leading operators (e.g., Vodafone, IpT/Telefonica, MTN, Zain, Etisalat, Cellcom, Inland Cellular, OptimEra, Optus) worldwide. Parallel Wireless's innovation and excellence in multi-technology, open virtualized RAN solutions have been recognized with 72+ industry awards.

In February 2020, Parallel Wireless won two GLOMO awards. The first was "best mobile infrastructure for global Open RAN deployments with Vodafone and TIP



for its solutions deployed in Turkey and the Democratic Republic of Congo (DRC). Vodafone will now roll out the Parallel Wireless solution across Europe. The second award was for its Open RAN Controller and Network Software Suite as best network software breakthrough.

For more details, go to www.parallelwireless.com.



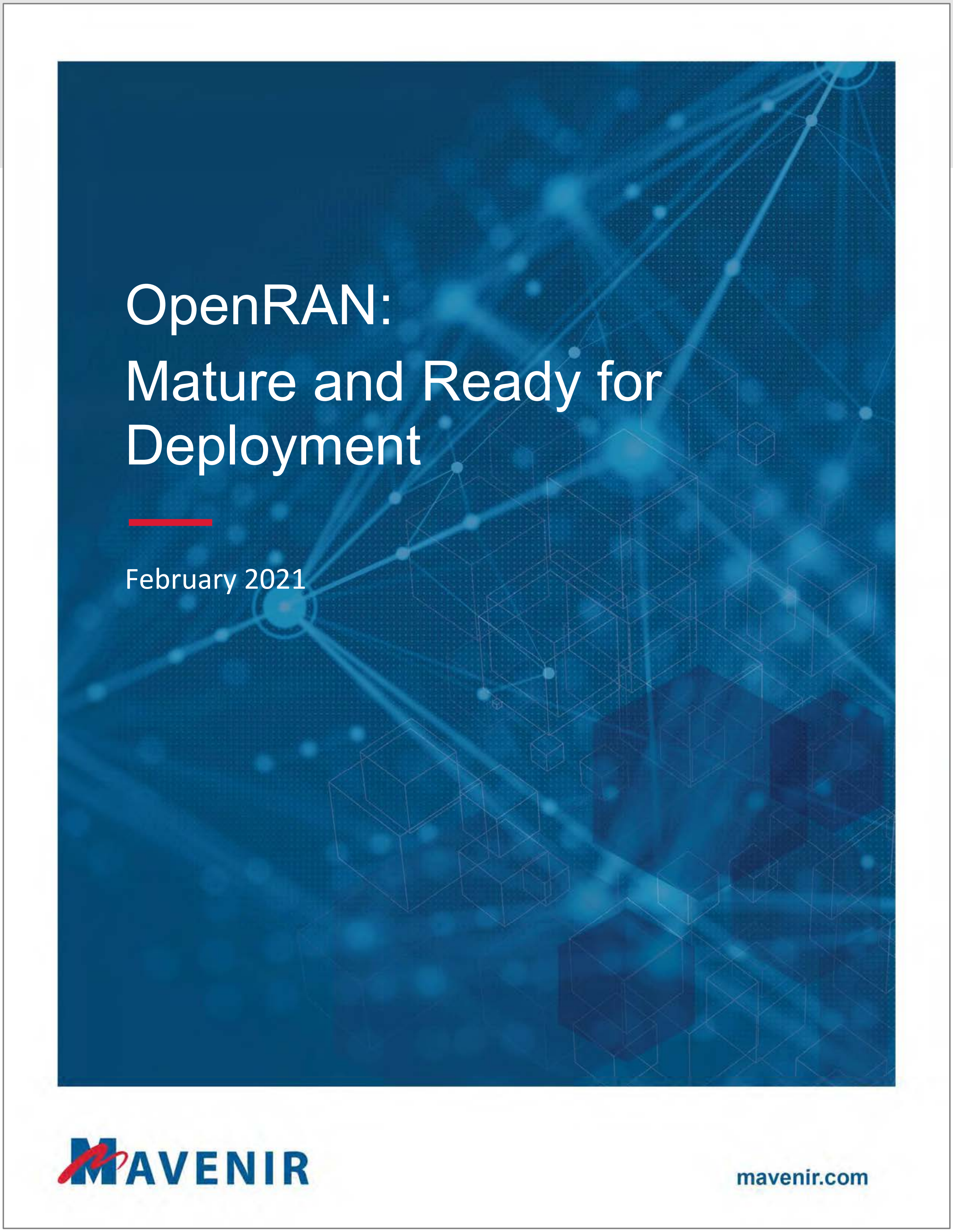
About *i*GR

*i*GR is a market strategy consultancy focused on the wireless and mobile communications industry. Founded by Iain Gillott, one of the wireless industry's leading analysts, we research and analyze the impact new wireless and mobile technologies will have on the industry, on vendors' competitive positioning, and on our clients' strategic business plans.

A more complete profile of the company can be found at http://www.iGR-inc.com/.

Disclaimer

The opinions expressed in this white paper are those of *i*GR and do not reflect the opinions of the companies or organizations referenced in this paper. All research was conducted exclusively and independently by *i*GR. This paper was supported by Altiostar, Mavenir and Parallel Wireless.

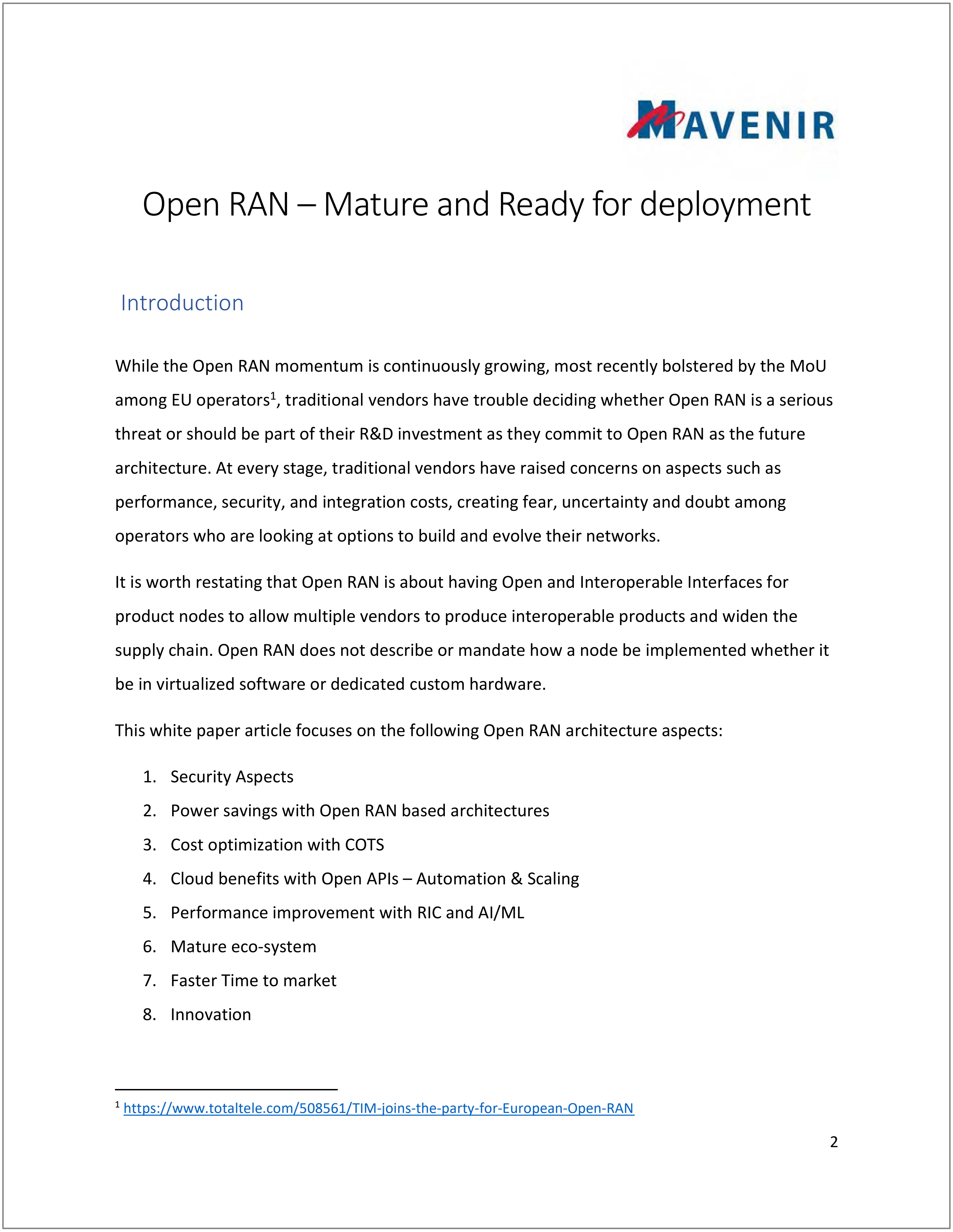


OpenRAN:
Mature and Ready for Deployment

February 2021

MAVENIR

mavenir.com



Open RAN – Mature and Ready for deployment

Introduction

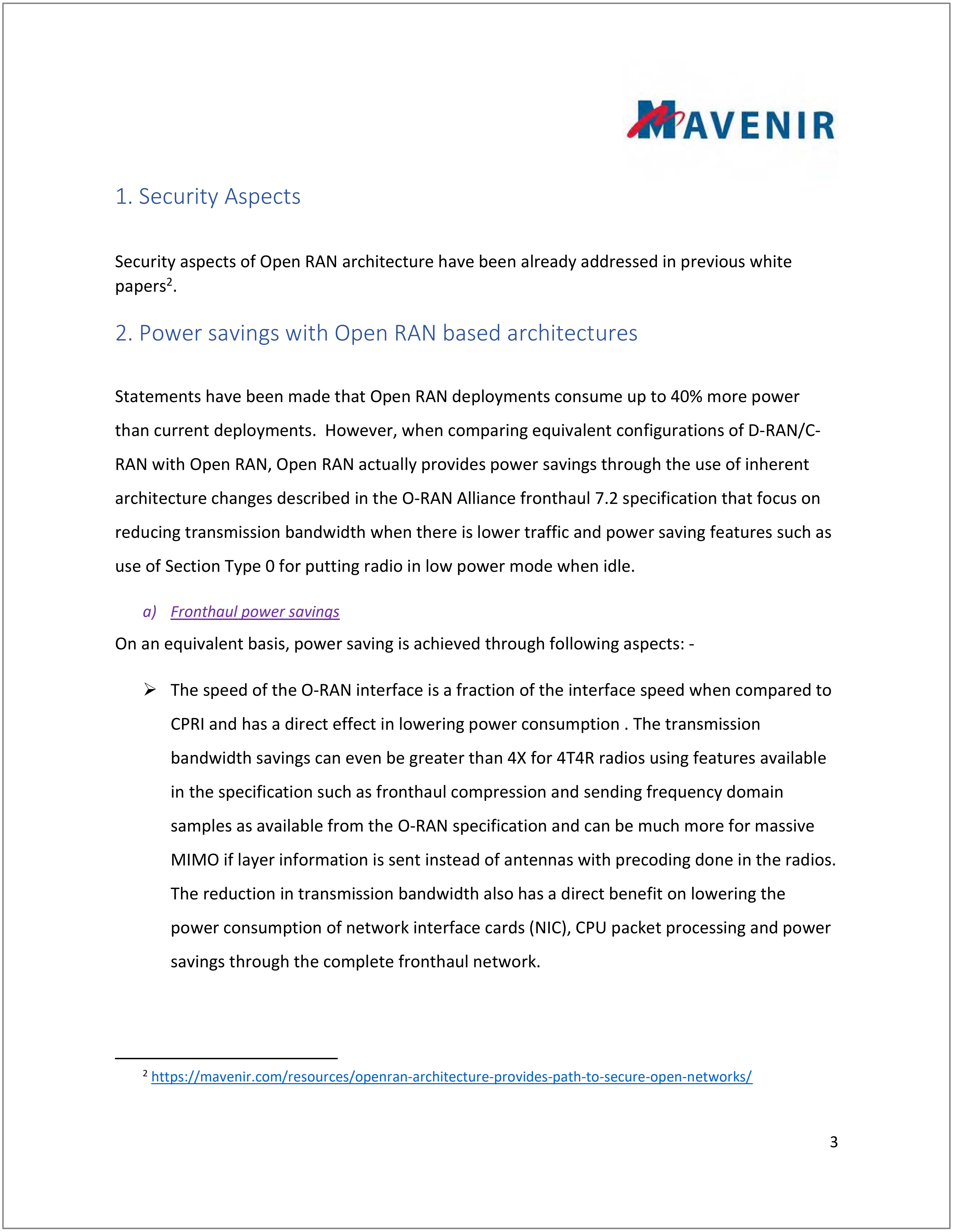
While the Open RAN momentum is continuously growing, most recently bolstered by the MoU among EU operators[1], traditional vendors have trouble deciding whether Open RAN is a serious threat or should be part of their R&D investment as they commit to Open RAN as the future architecture. At every stage, traditional vendors have raised concerns on aspects such as performance, security, and integration costs, creating fear, uncertainty and doubt among operators who are looking at options to build and evolve their networks.

It is worth restating that Open RAN is about having Open and Interoperable Interfaces for product nodes to allow multiple vendors to produce interoperable products and widen the supply chain. Open RAN does not describe or mandate how a node be implemented whether it be in virtualized software or dedicated custom hardware.

This white paper article focuses on the following Open RAN architecture aspects:

1. Security Aspects
2. Power savings with Open RAN based architectures
3. Cost optimization with COTS
4. Cloud benefits with Open APIs – Automation & Scaling
5. Performance improvement with RIC and AI/ML
6. Mature eco-system
7. Faster Time to market
8. Innovation

[1] https://www.totaltele.com/508561/TIM-joins-the-party-for-European-Open-RAN



1. Security Aspects

Security aspects of Open RAN architecture have been already addressed in previous white papers[2].

2. Power savings with Open RAN based architectures

Statements have been made that Open RAN deployments consume up to 40% more power than current deployments. However, when comparing equivalent configurations of D-RAN/C-RAN with Open RAN, Open RAN actually provides power savings through the use of inherent architecture changes described in the O-RAN Alliance fronthaul 7.2 specification that focus on reducing transmission bandwidth when there is lower traffic and power saving features such as use of Section Type 0 for putting radio in low power mode when idle.

a) Fronthaul power savings

On an equivalent basis, power saving is achieved through following aspects: -

- The speed of the O-RAN interface is a fraction of the interface speed when compared to CPRI and has a direct effect in lowering power consumption . The transmission bandwidth savings can even be greater than 4X for 4T4R radios using features available in the specification such as fronthaul compression and sending frequency domain samples as available from the O-RAN specification and can be much more for massive MIMO if layer information is sent instead of antennas with precoding done in the radios. The reduction in transmission bandwidth also has a direct benefit on lowering the power consumption of network interface cards (NIC), CPU packet processing and power savings through the complete fronthaul network.

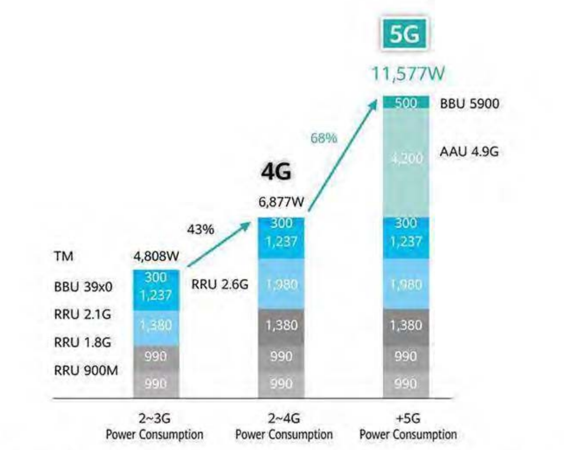
[2] https://mavenir.com/resources/openran-architecture-provides-path-to-secure-open-networks/

- As designed in the O-RAN front haul interface specification, the used transmission bandwidth is proportional to the user bandwidth. If there is zero traffic, there is minimal front haul interface traffic allowing the power consumption to be minimized.
- With no traffic, the DU draws minimal power and uses minimal CPU core resources due to minimal traffic. This allows the DU to be overprovisioned supporting multiple RRUs per DU eliminating dedicated DU's per radio given step functions in power savings.

b) RF power savings

The RF dominates the power consumption at a cell site for 5G as shown in the figure below from Huawei. Open RAN interfaces do not impact the radio (RF) power consumption. The RF power consumption is not impacted by the interface since the radio only performs time domain processing and uses optimized fronthaul. The Open RAN ecosystem is growing through white box radio developments such as Evenstar with Facebook, MTI and Mavenir. With the removal of margin stacking, licenses structure and the saving in power consumption through RF device innovation, the radio cost can come down substantially. There have been multiple announcements by Analog Devices, Maxlinear, Fujitsu, MTI and others related to innovative DPD/CFR techniques. Such innovation will be further strengthened by the entry of multiple new players in the Open RAN ecosystem. The power savings of radios with Open RAN based split 7 architectures has also been demonstrated by NEC in their Rakuten deployment[3].

[3] https://www.nec.com/en/press/202003/global_20200324_02.html



Typical maximum power consumption of a single 5G base station

Source: Huawei[4]

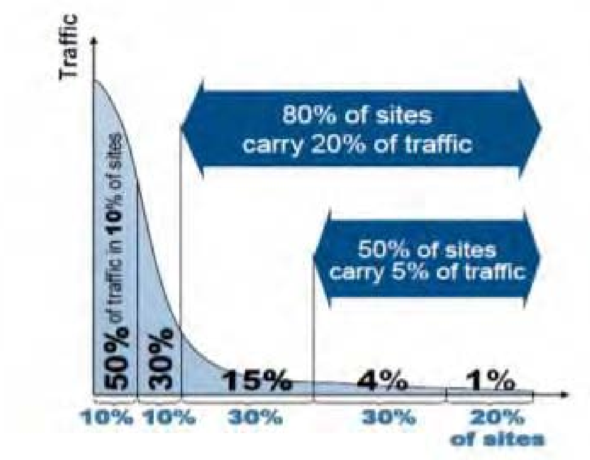
c) *RAN software power savings.*

As the disaggregated RAN compute resources move to data centers, the power efficiency can take advantage of the global data center power optimization trends. The data center power consumption has increased by 6% since 2010 but at same time the amount of compute in the data center has increased by 550%[4]. With centralized baseband processing in the cloud, it is much easier to pool resources taking into account the workload variations across cell sites and time of day and implement usage-based power savings that can be adjusted dynamically. A NGMN study in Europe shows that 80% of a wireless network carry only 20% of the traffic.[5] and pooling across sites could potentially reduce DU/CU capacity requirements with significant compute and power savings. With scalability and demand-based usage, processors (CPUs or GPUs) that are processing radio software can also run other applications during non-peak times. This is

[4] https://www.datacenters.com/news/data-center-power-optimization-increase-efficiency-with-a-data-center-audit

[5] https://www.ngmn.org/wp-content/uploads/NGMN_RANEV_D2_Further_Study_on_Critical_C-RAN_Technologes_v1.0.pdf

not possible with proprietary baseband systems using dedicated, non-reusable hardware.

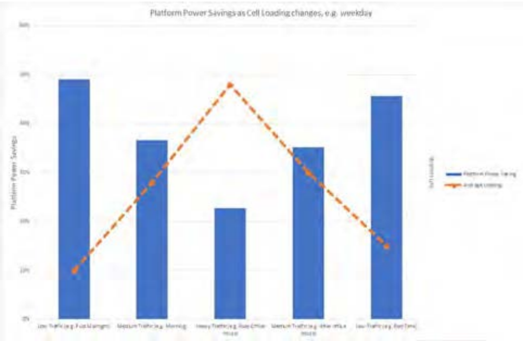


Source: NGMN[5]

d) Platform Power Savings with load

Moving RAN to the cloud using open interfaces offers potential reduction of electricity cost, as the RAN processing can now be shared among cell sites. In densely deployed networks, as in city centers, the network traffic load can fluctuate very much during the day, with significant periods of minimal traffic at certain cell sites for extended periods. There are also many short gaps in the data transmissions even during highly loaded times. Modelling the cell load profile over a 24-hour period over different types of cells, demonstrates that power savings in the range of 30-55% can be achieved.

.

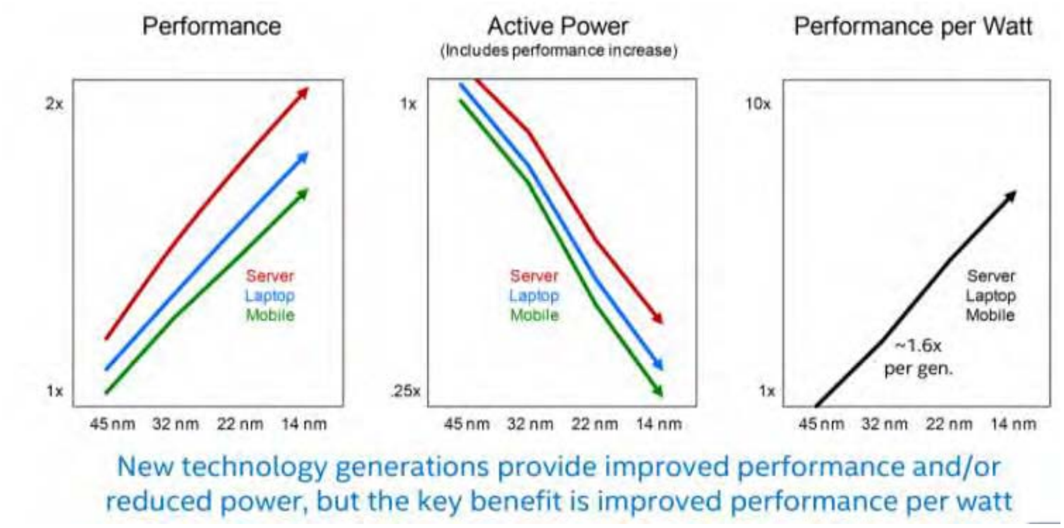


Elastic Power Savings

Advanced measurements using AI/ML can be performed to predict traffic patterns, traffic load, and end-user needs, from network level across nodes down to subframe levels with a cell. Based on this data, RAN compute and radio equipment can be dynamically activated to achieve the lowest possible energy consumption with maintained network performance. The dynamic compute provisioning optimizes utilization of silicon and prevents over-provisioning of resources. This results in reduction in power and energy consumption compared to traditional RAN architecture, improves scalability, and consequentially lowers the TCO.

This consolidation also enables telco operators to take advantage of existing compute and storage infrastructure offered by cloud providers, instead of incurring all such costs in-house. A public cloud hosted deployment will significantly reduce the investment burden on telco operators.

When looking at processor roadmaps, power efficiency and capacity is improved with every generation of the processor technology providing performance improvements as the transistor feature size continues to shrink. Also, further optimizations are possible for dynamic power management using processor BIOS and power settings to control the voltage and frequency of the processor based on the network configuration and usage. The figure below shows roughly a 1.6X improvement in performance per watt every processor generation.



New technology generations provide improved performance and/or reduced power, but the key benefit is improved performance per watt

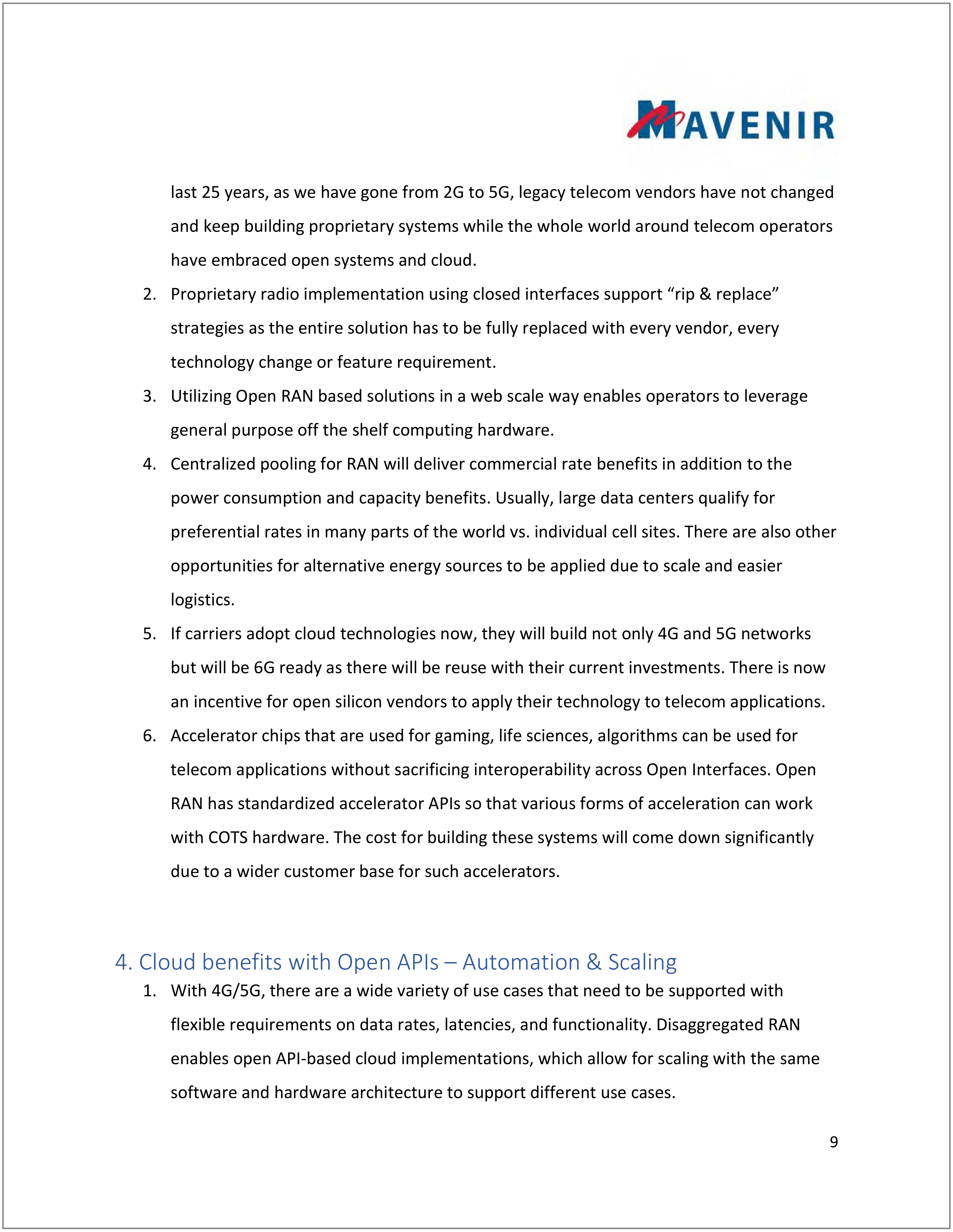
Source: Intel

d) *Accelerator power savings*

To restate, just because RAN is now open – dedicated hardware can still be used for specialized functions for performance and power saving improvements. – ***Open RAN simply implies interfaces are open***. Though the preference is for COTS hardware from a reuse preference, dedicated (e)ASICs, FPGAs, GPUs, and other such commercially open accelerators, are perfectly acceptable solutions to provide hardware function acceleration and power savings in the context of open RAN. The performance and power optimizations on these accelerators are also rapidly improving with every generation as they address the telecom market, and they are being made more generic to support a wider variety of applications with the same hardware.

3. Cost optimization with cloud and COTS

1. Operators throw away proprietary systems from traditional vendors every few years and are unable to use these proprietary radio systems for any other application. In the

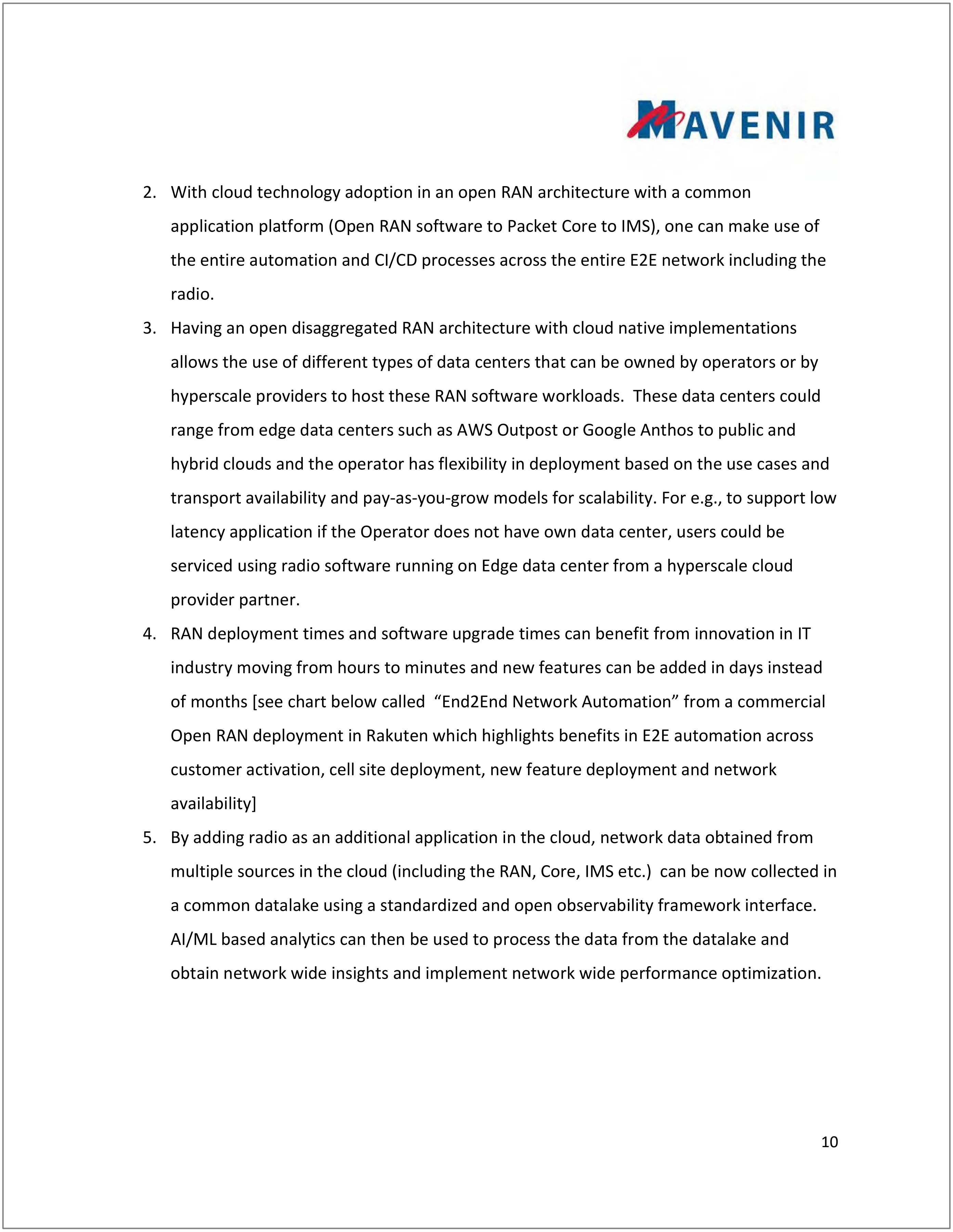


last 25 years, as we have gone from 2G to 5G, legacy telecom vendors have not changed and keep building proprietary systems while the whole world around telecom operators have embraced open systems and cloud.

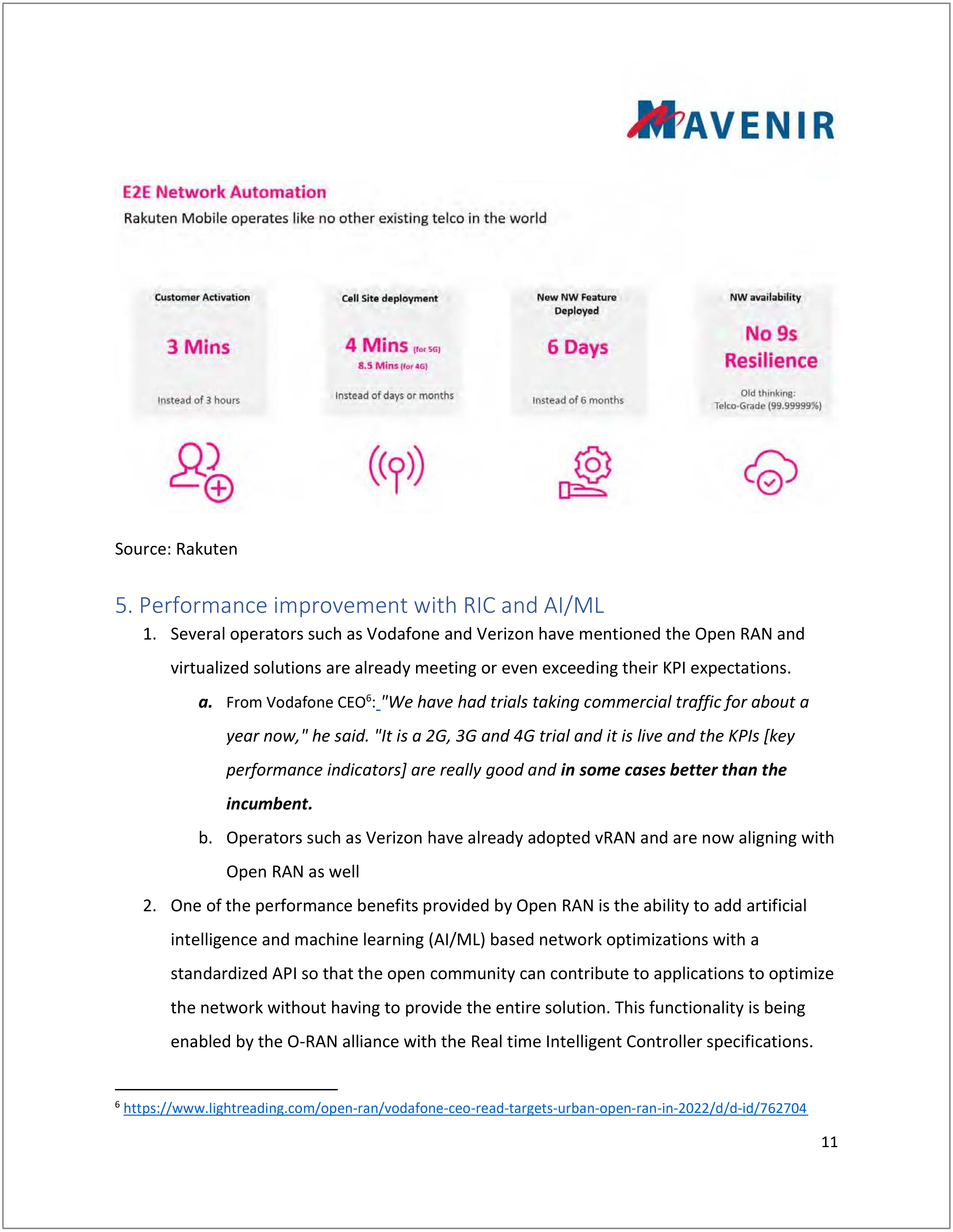
2. Proprietary radio implementation using closed interfaces support “rip & replace” strategies as the entire solution has to be fully replaced with every vendor, every technology change or feature requirement.
3. Utilizing Open RAN based solutions in a web scale way enables operators to leverage general purpose off the shelf computing hardware.
4. Centralized pooling for RAN will deliver commercial rate benefits in addition to the power consumption and capacity benefits. Usually, large data centers qualify for preferential rates in many parts of the world vs. individual cell sites. There are also other opportunities for alternative energy sources to be applied due to scale and easier logistics.
5. If carriers adopt cloud technologies now, they will build not only 4G and 5G networks but will be 6G ready as there will be reuse with their current investments. There is now an incentive for open silicon vendors to apply their technology to telecom applications.
6. Accelerator chips that are used for gaming, life sciences, algorithms can be used for telecom applications without sacrificing interoperability across Open Interfaces. Open RAN has standardized accelerator APIs so that various forms of acceleration can work with COTS hardware. The cost for building these systems will come down significantly due to a wider customer base for such accelerators.

4. Cloud benefits with Open APIs – Automation & Scaling

1. With 4G/5G, there are a wide variety of use cases that need to be supported with flexible requirements on data rates, latencies, and functionality. Disaggregated RAN enables open API-based cloud implementations, which allow for scaling with the same software and hardware architecture to support different use cases.



2. With cloud technology adoption in an open RAN architecture with a common application platform (Open RAN software to Packet Core to IMS), one can make use of the entire automation and CI/CD processes across the entire E2E network including the radio.
3. Having an open disaggregated RAN architecture with cloud native implementations allows the use of different types of data centers that can be owned by operators or by hyperscale providers to host these RAN software workloads. These data centers could range from edge data centers such as AWS Outpost or Google Anthos to public and hybrid clouds and the operator has flexibility in deployment based on the use cases and transport availability and pay-as-you-grow models for scalability. For e.g., to support low latency application if the Operator does not have own data center, users could be serviced using radio software running on Edge data center from a hyperscale cloud provider partner.
4. RAN deployment times and software upgrade times can benefit from innovation in IT industry moving from hours to minutes and new features can be added in days instead of months [see chart below called "End2End Network Automation" from a commercial Open RAN deployment in Rakuten which highlights benefits in E2E automation across customer activation, cell site deployment, new feature deployment and network availability]
5. By adding radio as an additional application in the cloud, network data obtained from multiple sources in the cloud (including the RAN, Core, IMS etc.) can be now collected in a common datalake using a standardized and open observability framework interface. AI/ML based analytics can then be used to process the data from the datalake and obtain network wide insights and implement network wide performance optimization.



E2E Network Automation

Rakuten Mobile operates like no other existing telco in the world

Customer Activation	Cell Site deployment	New NW Feature Deployed	NW availability
3 Mins	4 Mins (for 5G) 8.5 Mins (for 4G)	6 Days	No 9s Resilience
Instead of 3 hours	Instead of days or months	Instead of 6 months	Old thinking: Telco-Grade (99.99999%)

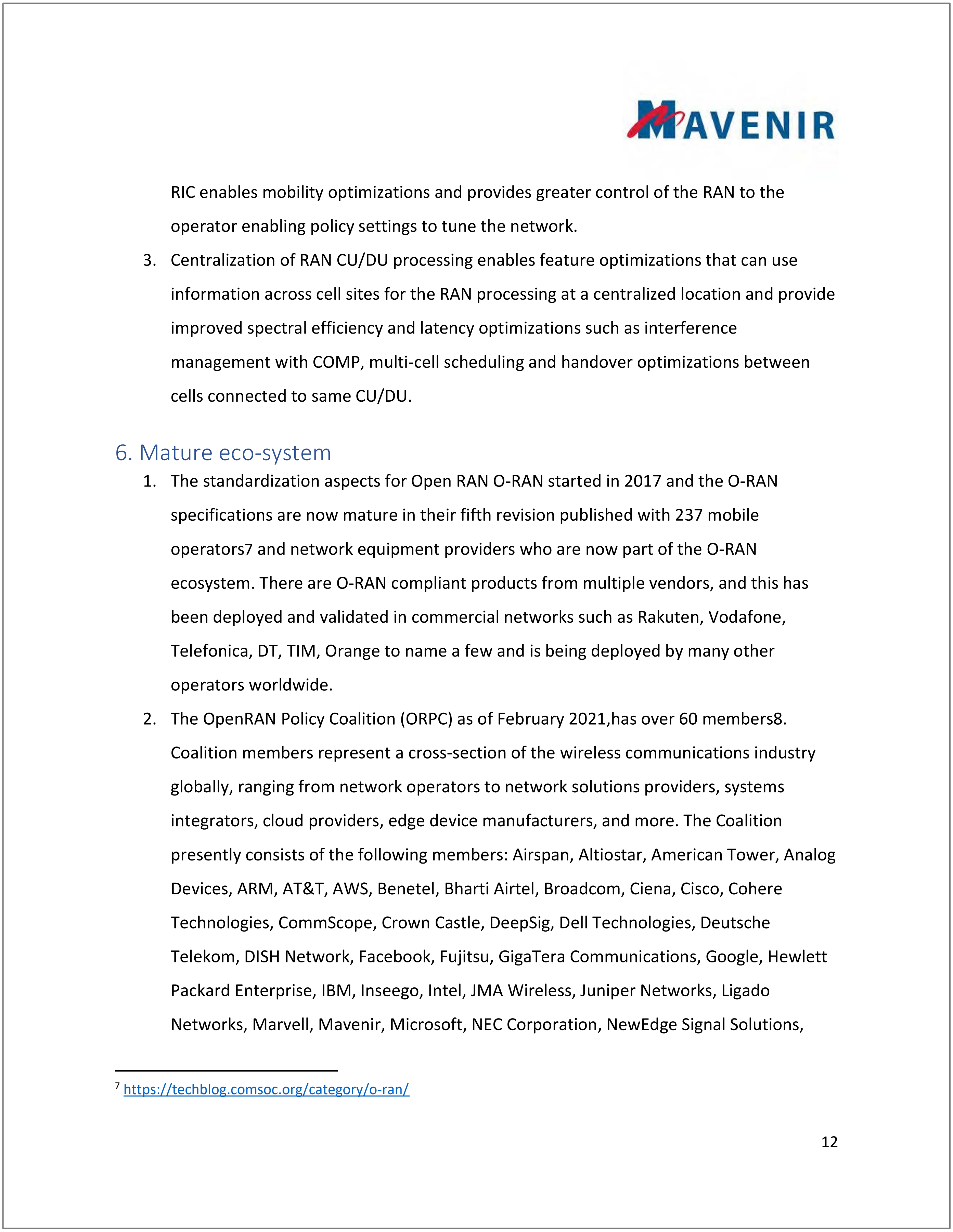
Source: Rakuten

5. Performance improvement with RIC and AI/ML

1. Several operators such as Vodafone and Verizon have mentioned the Open RAN and virtualized solutions are already meeting or even exceeding their KPI expectations.
   - ***a.*** From Vodafone CEO[6]: *"We have had trials taking commercial traffic for about a year now," he said. "It is a 2G, 3G and 4G trial and it is live and the KPIs [key performance indicators] are really good and* ***in some cases better than the incumbent.***
   - b. Operators such as Verizon have already adopted vRAN and are now aligning with Open RAN as well
2. One of the performance benefits provided by Open RAN is the ability to add artificial intelligence and machine learning (AI/ML) based network optimizations with a standardized API so that the open community can contribute to applications to optimize the network without having to provide the entire solution. This functionality is being enabled by the O-RAN alliance with the Real time Intelligent Controller specifications.

[6] https://www.lightreading.com/open-ran/vodafone-ceo-read-targets-urban-open-ran-in-2022/d/d-id/762704

11



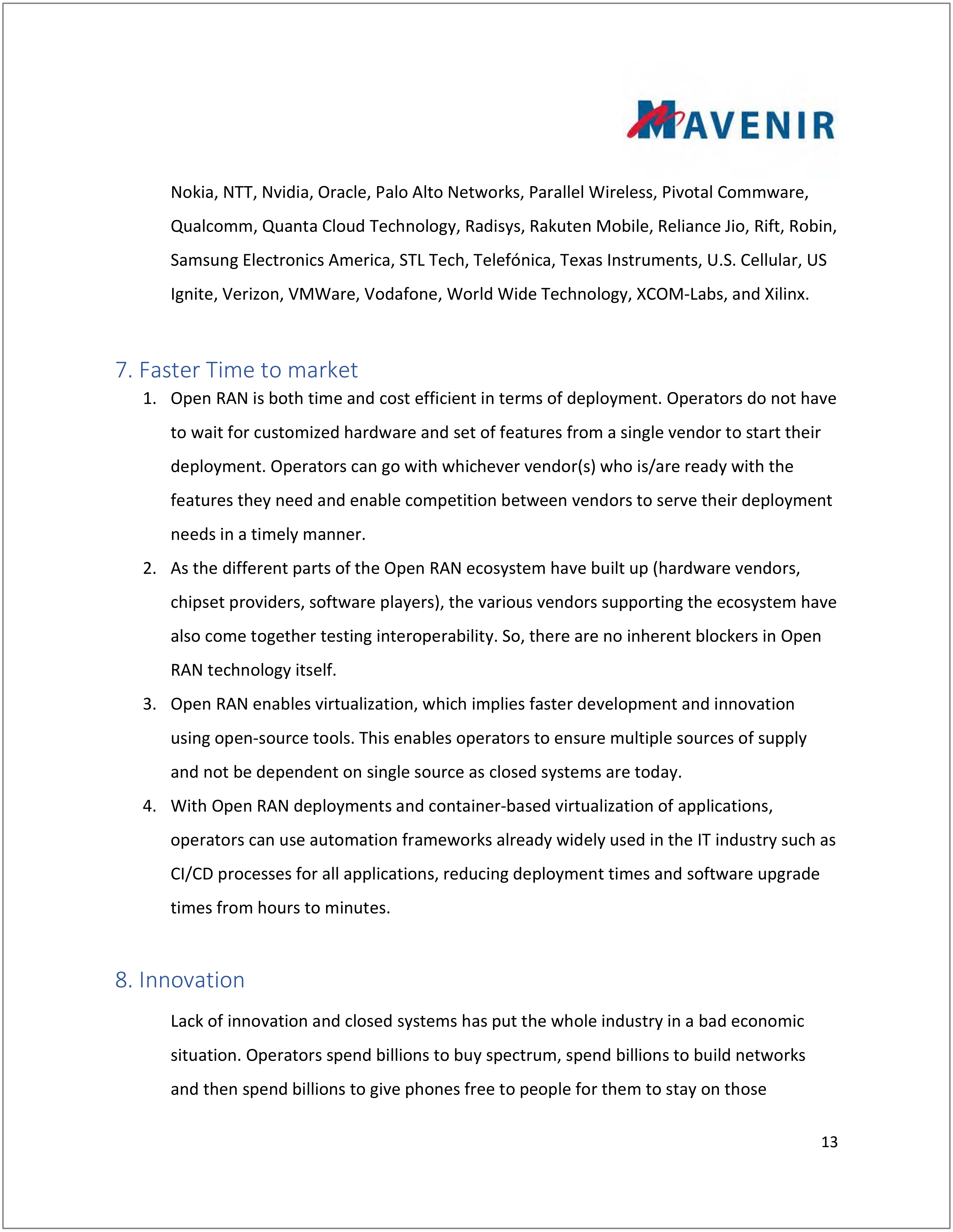
RIC enables mobility optimizations and provides greater control of the RAN to the operator enabling policy settings to tune the network.

3. Centralization of RAN CU/DU processing enables feature optimizations that can use information across cell sites for the RAN processing at a centralized location and provide improved spectral efficiency and latency optimizations such as interference management with COMP, multi-cell scheduling and handover optimizations between cells connected to same CU/DU.

6. Mature eco-system

1. The standardization aspects for Open RAN O-RAN started in 2017 and the O-RAN specifications are now mature in their fifth revision published with 237 mobile operators7 and network equipment providers who are now part of the O-RAN ecosystem. There are O-RAN compliant products from multiple vendors, and this has been deployed and validated in commercial networks such as Rakuten, Vodafone, Telefonica, DT, TIM, Orange to name a few and is being deployed by many other operators worldwide.
2. The OpenRAN Policy Coalition (ORPC) as of February 2021,has over 60 members8. Coalition members represent a cross-section of the wireless communications industry globally, ranging from network operators to network solutions providers, systems integrators, cloud providers, edge device manufacturers, and more. The Coalition presently consists of the following members: Airspan, Altiostar, American Tower, Analog Devices, ARM, AT&T, AWS, Benetel, Bharti Airtel, Broadcom, Ciena, Cisco, Cohere Technologies, CommScope, Crown Castle, DeepSig, Dell Technologies, Deutsche Telekom, DISH Network, Facebook, Fujitsu, GigaTera Communications, Google, Hewlett Packard Enterprise, IBM, Inseego, Intel, JMA Wireless, Juniper Networks, Ligado Networks, Marvell, Mavenir, Microsoft, NEC Corporation, NewEdge Signal Solutions,

[7] https://techblog.comsoc.org/category/o-ran/



Nokia, NTT, Nvidia, Oracle, Palo Alto Networks, Parallel Wireless, Pivotal Commware, Qualcomm, Quanta Cloud Technology, Radisys, Rakuten Mobile, Reliance Jio, Rift, Robin, Samsung Electronics America, STL Tech, Telefónica, Texas Instruments, U.S. Cellular, US Ignite, Verizon, VMWare, Vodafone, World Wide Technology, XCOM-Labs, and Xilinx.

7. Faster Time to market

1. Open RAN is both time and cost efficient in terms of deployment. Operators do not have to wait for customized hardware and set of features from a single vendor to start their deployment. Operators can go with whichever vendor(s) who is/are ready with the features they need and enable competition between vendors to serve their deployment needs in a timely manner.
2. As the different parts of the Open RAN ecosystem have built up (hardware vendors, chipset providers, software players), the various vendors supporting the ecosystem have also come together testing interoperability. So, there are no inherent blockers in Open RAN technology itself.
3. Open RAN enables virtualization, which implies faster development and innovation using open-source tools. This enables operators to ensure multiple sources of supply and not be dependent on single source as closed systems are today.
4. With Open RAN deployments and container-based virtualization of applications, operators can use automation frameworks already widely used in the IT industry such as CI/CD processes for all applications, reducing deployment times and software upgrade times from hours to minutes.

8. Innovation

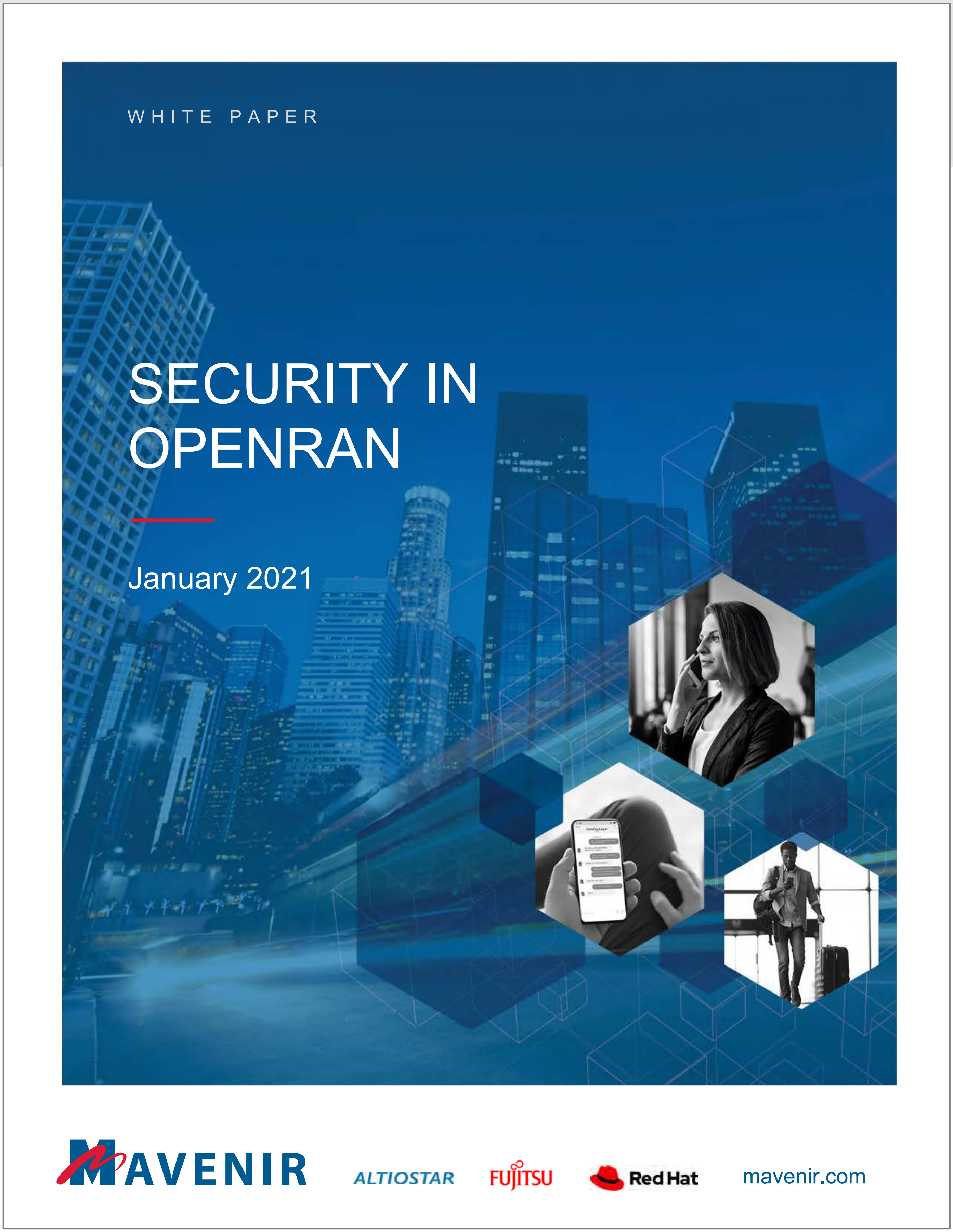
Lack of innovation and closed systems has put the whole industry in a bad economic situation. Operators spend billions to buy spectrum, spend billions to build networks and then spend billions to give phones free to people for them to stay on those networks. There is no money left to do anything innovative. Companies like Zoom, Twilio, Snap chat and many others make money running on these networks.

Open RAN also enables open-source eco-system for development. A comparison can be made with Linux and Microsoft, when it was mentioned that open-source software will make all applications on that platform open source and unusable, which turned out to be false[8]. ***The key is Open Interfaces.*** Open RAN, by enabling open APIs, enables innovation, while allowing vendors to differentiate within the applications and functionality provided by their hardware and software.

1. Having an Open RAN architecture now enables multiple vendors and operators to co-operate, contribute and innovate on new technologies as the industry moves towards 6G.

For more information, visit www.mavenir.com

[8] https://www.theregister.com/2001/06/02/ballmer_linux_is_a_cancer/



WHITE PAPER

SECURITY IN OPENRAN

January 2021

MAVENIR ALTIOSTAR FUJITSU Red Hat mavenir.com

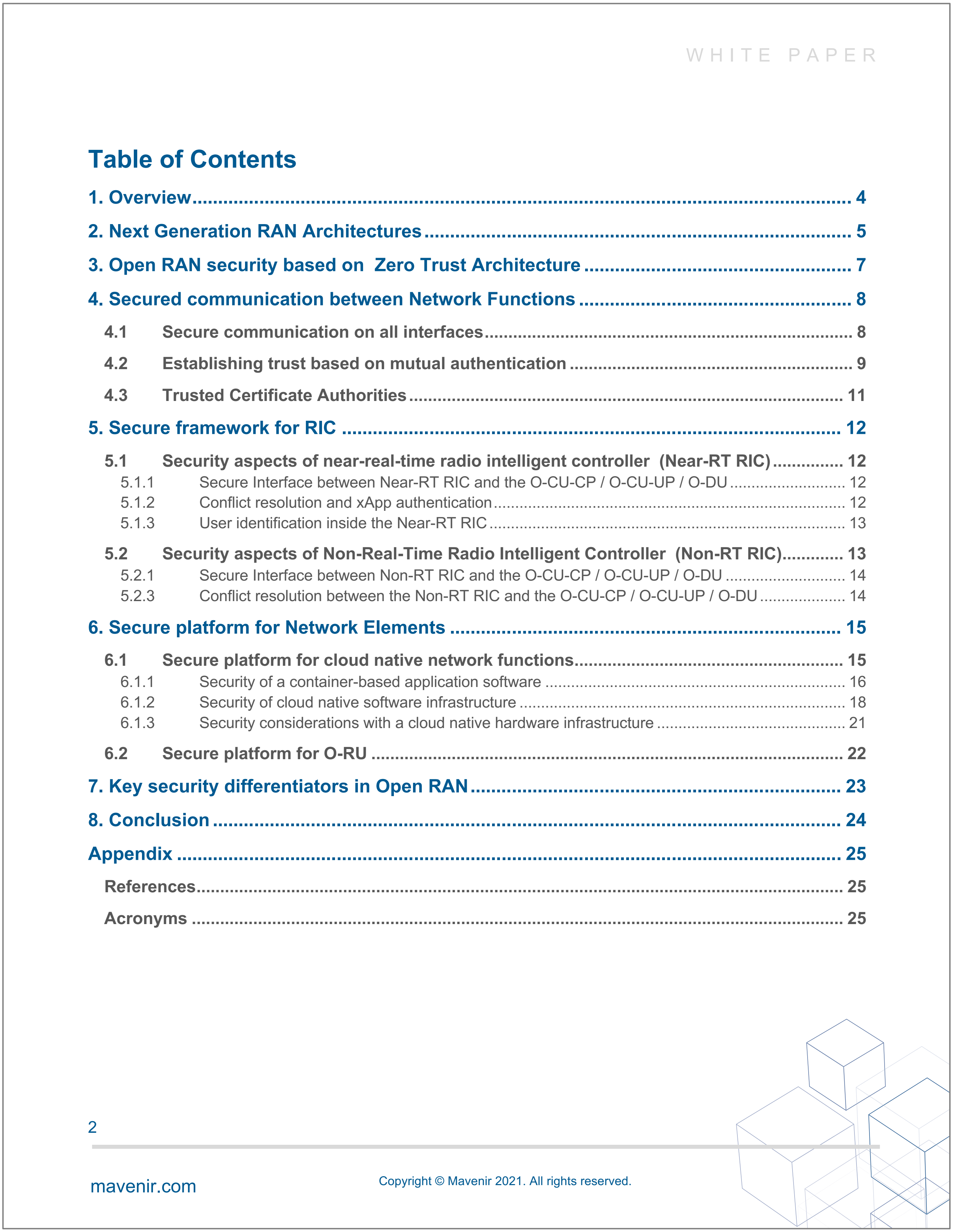


Table of Contents

Table of Figures

Definitions

Network Service (NS): A composition of network functions defined by its functional and behavioral specification. In the RAN Context, a gNB is a Network Service.

Network Function (NF): A functional building block within a Network Service, with well-defined interfaces and behavior. In the O-RAN Alliance's RAN architecture context, a O-DU, O-CU-CP, O-CU-UP, Near-RT RIC and Non-RT RIC are Network Functions.

Cloud Native Network Function (CNF): CNF is one type of manifestation of a NF (like VNF or PNF) deployed as a decomposed set of containerized

microservices. In a cloud native realization of O-RAN Alliance's RAN architecture, the managed entities, O-CU-CP, O-CU-UP, O-DU, Near-RT RIC, Non-RT RIC and Service Management and Orchestration (SMO) are CNFs. CNF and NF are interchangeable in the context of 5G cloud native services.

Physical Network Function (PNF): This refers to network functions that are not virtualized. In the O-RAN Alliance's RAN architecture context, the O-RUs that are deployed at a cell site can be considered PNFs.

1. Overview

Open RAN is an open radio access network (RAN) architecture standardized by the O-RAN Alliance based on 3GPP and other standards. O-RAN Alliance's RAN functional split is based on the three key tenets:

- Decoupling of hardware and software
- Cloud infrastructure
- Standardized and open interfaces between the network functions

In the IT world, hardware-software decoupling happened a long time ago. This decoupling led to the emergence of software players that were experts in specific horizontal layers. The software from these players could run on any hardware providing operator customers with a variety of options. An equally rich ecosystem of hardware players emerged.

Virtualization technologies have helped enterprises reduce their TCO through efficient use of compute resources, removal of hardware silos and increased automation. To deliver 5G services, operators need a virtualized network capable of scaling services based on policy-driven service selections for subscribers. Cloud native architecture allows deployment of network functions (NFs) as a cluster of containerized microservices, where each microservice can be deployed, scaled, and upgraded independently. Instead of scaling the whole application, only the required component within the NF is scaled.

Open interfaces between various network functions allow best of breed equipment to be used in networks enabling operators to distinguish themselves from competition by using bespoke network functions, as needed.

In this paper it is demonstrated how, by adopting a zero-trust security framework, an Open RAN architecture provides a path to a more secure open networks and open interfaces over what exists today. Despite misconceptions, open interfaces, defined in the O-RAN technical specifications, provide increased independent visibility and the opportunity for an overall enhanced and more secure system.

5G and Open RAN enable new capabilities and control points that allow suppliers, test equipment manufacturers, wireless carriers, and network operators to assess, mitigate and manage security risks efficiently. This paper details how O-RAN enables operators with full visibility and control of their network's end-to-end security.

There is a vast cloud industry solving security issues, and cloud RAN network functions are similar to other cloud network functions, with similar security requirements and solutions. Cloud architecture ensures resilience, scalability and segmentation and the introduction of features such as AI/ML and Multi-Access Edge Computing (MEC). For example, leveraging MEC, allows collection and processing of sensor traffic at a factory to shift DDoS detection and mitigation to the edge of the network where incidents at the edge can be isolated from the rest of the network. Microsegmentation, containerization, virtualization, and network slicing provide enhanced security and isolation from the hardware up. The security measures are designed into the system rather than being bolted on afterwards as in traditional systems.

2. Next Generation RAN Architectures

3GPP [1] has defined the following architecture for 5G NR gNB as shown in **Figure 1.**

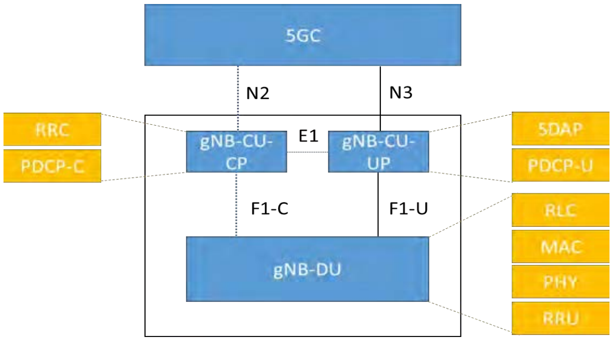


Figure 1: gNB Logical Architecture in 3GPP

gNB is split into two logical functions called CU (Centralized Unit) and DU (Distributed Unit) as shown in **Figure 1** and these two entities are connected by F1-C and F1-U interfaces as defined in 3GPP TS 38.473[2]. It may be noted that the 3GPP architecture does not specify the Remote Radio Unit (RRU) i.e. the interface between PHY and RF layers is left to vendor implementation.

O-RAN Alliance, a group of leading vendors and operators defining Open RAN specifications, further disaggregate CU and DU network functions [3] as defined by 3GPP that are inter-connected over open, standardized, secure interfaces as shown in **Figure 2**.

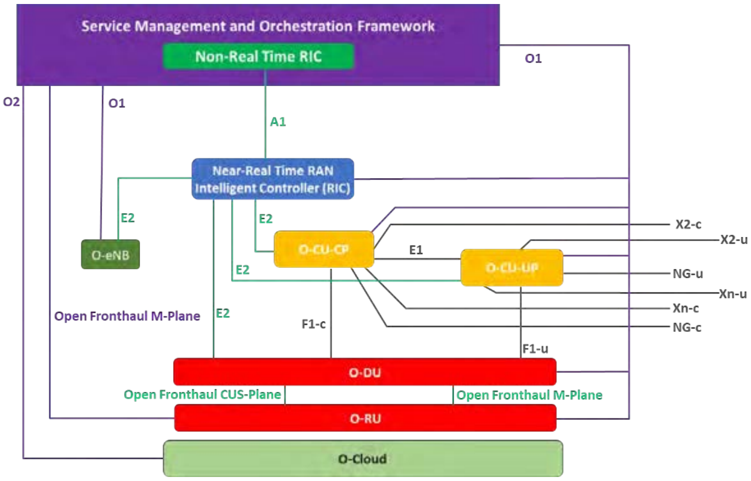


Figure 2: gNB Logical Architecture in O-RAN

Figure 3 shows the functional and interface split between 3GPP and O-RAN. The O-RAN Alliance adds new interfaces and functions beyond 3GPP's 5G RAN architecture.

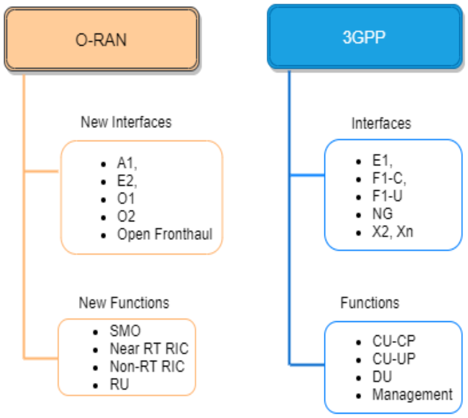


Figure 3: Interfaces and Functions split between O-RAN and 3GPP

Since O-RAN Alliance builds on 3GPP's 5G NR architecture, it benefits from 3GPP's advanced security features introduced for 5G [4] including:

- Enhanced user identity privacy i.e., Subscription Concealed Identifier (SUCI)
- Full protection of control/user plane traffic between the UE and gNB (encryption and integrity protection) over the air interface
- Full protection of gNB interfaces including the E1 interface between CU-CP and CU-UP and the F1 interface between CU and DU
- Enhanced home network control (authentication)
- Additional security for network slices based on SLA

3. Open RAN security based on Zero Trust Architecture

Rooted in the principle of “never trust, always verify,” Zero Trust is designed to protect modern digital environments by leveraging network segmentation, preventing lateral movement, providing Layer 7 threat prevention, and simplifying granular user-access control.

A zero trust architecture (ZTA) is a cybersecurity architecture that is based on zero trust principles and designed to prevent data breaches and limit internal lateral movement. The following is the relevant text from NIST publication 800-207 - ‘Zero Trust Architecture’ [5]-

A “zero trust” (ZT) approach to cybersecurity is primarily focused on data and service protection but can and should be expanded to include all enterprise assets (devices, infrastructure components, applications, virtual and cloud components) and subjects (end users, applications and other nonhuman entities that request information from resources).

In this new paradigm, an enterprise must assume no implicit trust and continually analyze and evaluate the risks to its assets and business functions and then enact protections to mitigate these risks. In zero trust, these protections usually involve minimizing access to resources (such as data and compute resources and applications/services) to only those subjects and assets identified as needing access as well as continually authenticating and authorizing the identity and security posture of each access request.

Support of a zero-trust architecture requires each O-RAN component to comply with established functionalities and protections. O-RAN Alliance [6] has identified several guiding principles for its ongoing work, including:

1. Support integration with an external identity, credential and access management system (ICAM) using industry standard protocols
2. Require authentication and authorization on all access
3. Support role-based access control (RBAC)
4. Implement confidentiality on connections between O-RAN and external components
5. Implement integrity checking on connections between O-RAN and external components
6. Support encryption of data at rest
7. Support replay prevention
8. Implement security log generation and collection to an external security information and event management (SIEM)

Open RAN security is built on the following tenets:

1. Secured communication between Network Functions
2. Secure framework for the Radio Intelligent Controller (RIC)
3. Secured platform for hosting the Network Functions

The analysis in the following sections assumes a cloud native Open RAN network with Network Functions modeled as containerized microservices.

4. Secured communication between Network Functions

This section explores following areas that relate to providing secure communication between all Network Functions in Open RAN.

a. Secure communication on all interfaces
b. Ensuring trust based authentication of communicating endpoints
c. Trusted Certificate Authorities for Identity Provisioning

4.1 Secure communication on all interfaces

O-RAN Alliance specifies an open and secure architecture that includes secure interfaces between all its components. Communications exchanged on these interfaces are cryptographically protected for encryption, integrity protection and replay protection.

Figure 4 depicts the 5G RAN network security architecture.

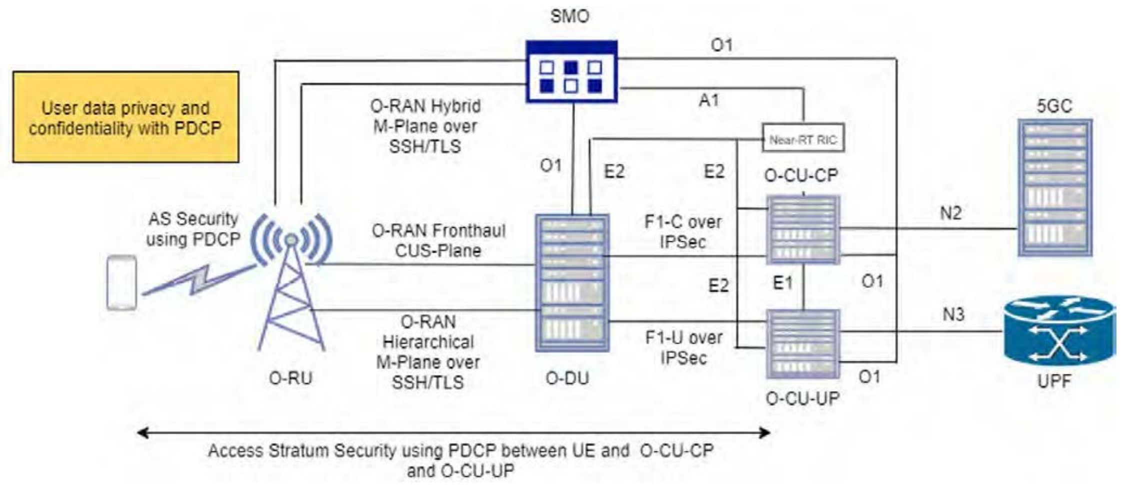
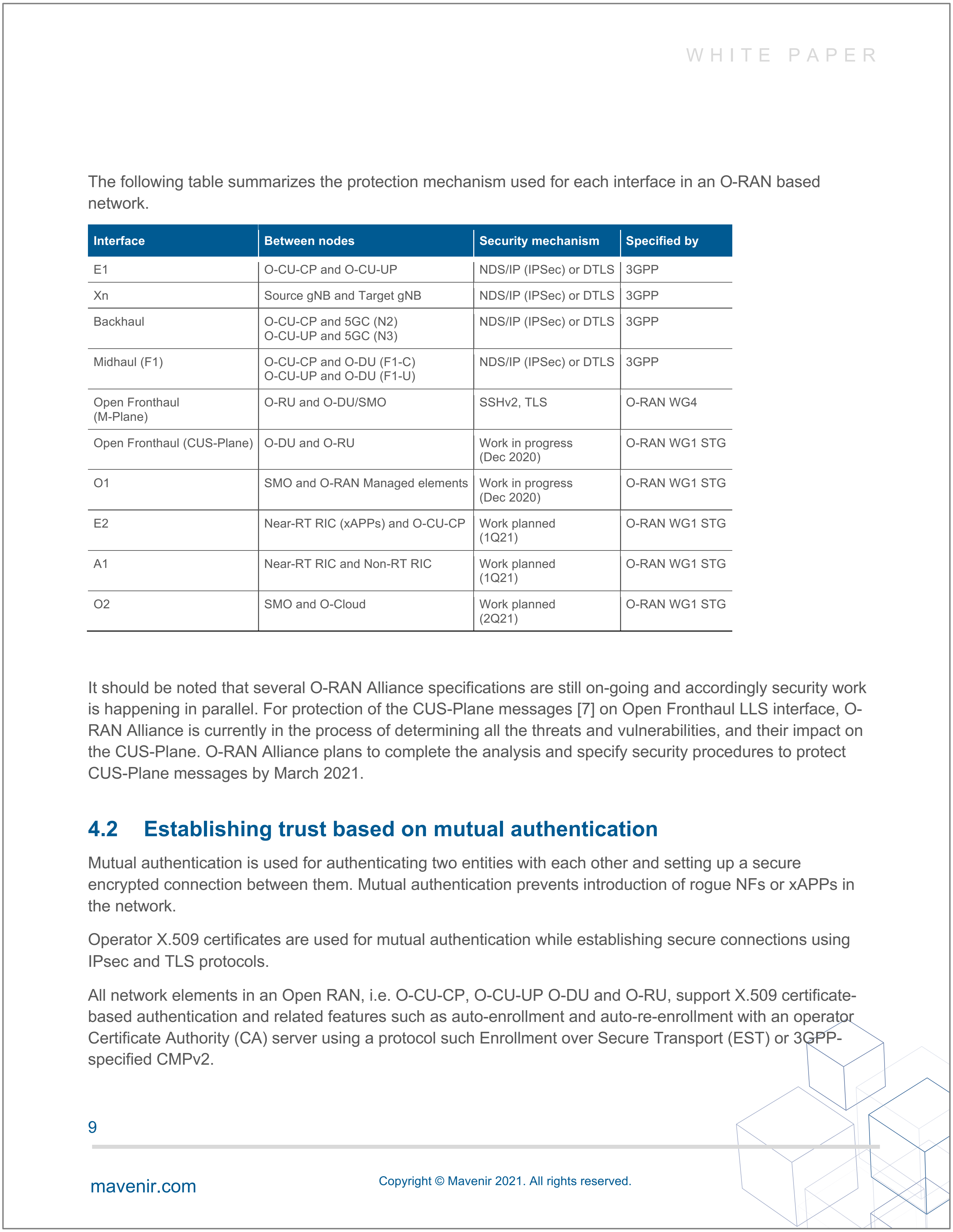

SMO
O1
A1
User data privacy and confidentiality with PDCP
O-RAN Hybrid M-Plane over SSH/TLS
5G C
Near-RT RIC
O1
E2
E2
O-CU-CP
AS Security using PDCP
O-RAN Fronthaul CUS-Plane
F1-C over IPSec
N2
E2
E1
O1
O-RAN Hierarchical M-Plane over SSH/TLS
F1-U over IPSec
N3
O-RU
O-DU
O1
UPF
O-CU-UP
Access Stratum Security using PDCP between UE and O-CU-CP and O-CU-UP

Figure 4: 5G RAN Network Security Architecture



The following table summarizes the protection mechanism used for each interface in an O-RAN based network.

Interface	Between nodes	Security mechanism	Specified by
E1	O-CU-CP and O-CU-UP	NDS/IP (IPSec) or DTLS	3GPP
Xn	Source gNB and Target gNB	NDS/IP (IPSec) or DTLS	3GPP
Backhaul	O-CU-CP and 5GC (N2) O-CU-UP and 5GC (N3)	NDS/IP (IPSec) or DTLS	3GPP
Midhaul (F1)	O-CU-CP and O-DU (F1-C) O-CU-UP and O-DU (F1-U)	NDS/IP (IPSec) or DTLS	3GPP
Open Fronthaul (M-Plane)	O-RU and O-DU/SMO	SSHv2, TLS	O-RAN WG4
Open Fronthaul (CUS-Plane)	O-DU and O-RU	Work in progress (Dec 2020)	O-RAN WG1 STG
O1	SMO and O-RAN Managed elements	Work in progress (Dec 2020)	O-RAN WG1 STG
E2	Near-RT RIC (xAPPs) and O-CU-CP	Work planned (1Q21)	O-RAN WG1 STG
A1	Near-RT RIC and Non-RT RIC	Work planned (1Q21)	O-RAN WG1 STG
O2	SMO and O-Cloud	Work planned (2Q21)	O-RAN WG1 STG

It should be noted that several O-RAN Alliance specifications are still on-going and accordingly security work is happening in parallel. For protection of the CUS-Plane messages [7] on Open Fronthaul LLS interface, O-RAN Alliance is currently in the process of determining all the threats and vulnerabilities, and their impact on the CUS-Plane. O-RAN Alliance plans to complete the analysis and specify security procedures to protect CUS-Plane messages by March 2021.

4.2 Establishing trust based on mutual authentication

Mutual authentication is used for authenticating two entities with each other and setting up a secure encrypted connection between them. Mutual authentication prevents introduction of rogue NFs or xAPPs in the network.

Operator X.509 certificates are used for mutual authentication while establishing secure connections using IPsec and TLS protocols.

All network elements in an Open RAN, i.e. O-CU-CP, O-CU-UP O-DU and O-RU, support X.509 certificate-based authentication and related features such as auto-enrollment and auto-re-enrollment with an operator Certificate Authority (CA) server using a protocol such Enrollment over Secure Transport (EST) or 3GPP-specified CMPv2.

The xAPPs in the Near-RT RIC are securely on-boarded like any other microservice and the O-RAN Alliance is expected to use CA signed X.509 certificates to authenticate before communicating over the E2 interface.

Figure 5 illustrates an example flow of how certificate-based authentication is used to authenticate an O-CU, O-DU and O-RU during certificate enrollment with a CA server.

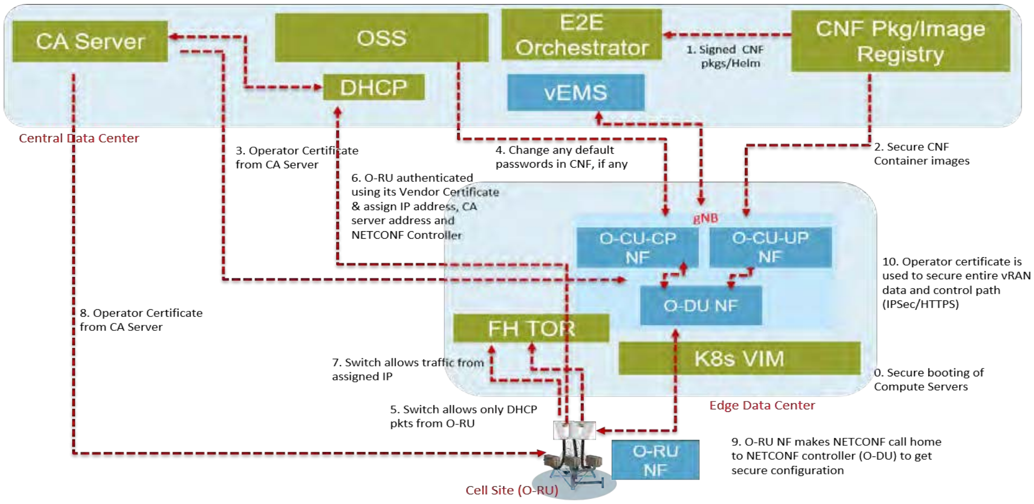

CA Server
OSS
E2E Orchestrator
CNF Pkg/Image Registry
1. Signed CNF pkgs/Helm
DHCP
vEMS
Central Data Center
3. Operator Certificate from CA Server
4. Change any default passwords in CNF, if any
2. Secure CNF Container images
6. O-RU authenticated using its Vendor Certificate & assign IP address, CA server address and NETCONF Controller
gNB
O-CU-CP NF
O-CU-UP NF
10. Operator certificate is used to secure entire vRAN data and control path (IPSec/HTTPS)
O-DU NF
8. Operator Certificate from CA Server
FH TOR
K8s VIM
7. Switch allows traffic from assigned IP
0. Secure booting of Compute Servers
Edge Data Center
5. Switch allows only DHCP pkts from O-RU
9. O-RU NF makes NETCONF call home to NETCONF controller (O-DU) to get secure configuration
O-RU NF
Cell Site (O-RU)

Figure 5: Certificate-based device authentication of O-CU, O-DU and O-RU

Step 1-2: *When the O-RU powers on, the O-CU-CP, O-CU-UP and O-DU instances that are allocated to serve that O-RU are instantiated by the orchestrator, if not already instantiated.*

Step 3: *an O-CU-CP, O-CU-UP and O-DU performs EST or a CMPv2-based certificate enrollment procedure in compliance with 3GPP with the CA server to obtain an operator certificate. The operator certificate is used for subsequent authentication when establishing an IPSec or a TLS connection.*

Step 4: *necessary OAM actions are performed on the O-CU, if any, including changing of default passwords.*

Steps 5 thru 9 *are executed as part of the O-RU power-on sequence. Key security related steps are explained below:*

- *The O-RU obtains its IP address, the EMS or OSS address from a DHCP server using one of the DHCP options specified in O-RAN M-Plane specification section 3.1.1 and 3.1.4 [8].*
- *The O-RU performs certificate enrollment procedure with the CA server to obtain an operator certificate. The vendor-provisioned device certificate is used for authenticating with the CA server.*

- *The O-RU shall notify the EMS or OSS with a NETCONF call home. O-RU's operator certificate is used to authenticate with the EMS. OSS / EMS shall configure the O-RU with the secondary NETCONF controller's address (i.e. the address of the O-DU).*
- *The O-RU shall notify the O-DU with a NETCONF call home to securely obtain O-RU's configuration. O-RU's operator certificate is used to authenticate with the O-DU.*

4.3 Trusted Certificate Authorities

It is recommended that the certificate authorities (CA) should be audited under the AICPA/CICA WebTrust Program for Certification Authorities.

This promotes confidence and trust in the CA servers used in Open RAN for authenticating network elements.

5. Secure framework for RIC

5.1 Security aspects of near-real-time radio intelligent controller (Near-RT RIC)

The Near-RT RIC is an SDN component that contains 3rd party extensible microservices (called xApps) that perform selected radio resource management (RRM) services for the NFs that were traditionally managed inside the gNB. The Near-RT RIC interfaces with the O-CU-CP, O-CU-UP and the O-DU via the O-RAN standardized open E2 interface. The Near-RT RIC also interfaces with the Non-RT RIC and the service management and orchestration framework via the A1 and O1 interfaces.

The key security aspects of the Near-RT RIC include:

- Secure E2 Interface between the Near-RT RIC and the O-CU-CP / O-CU-UP / O-DU
- Conflict resolution and xApp authentication
- User identification inside the Near-RT RIC

5.1.1 Secure Interface between Near-RT RIC and the O-CU-CP / O-CU-UP / O-DU

Interface security is explained in § 4.2

5.1.2 Conflict resolution and xApp authentication

The conflict resolution among the xApps is not necessarily a security issue but can lead to vulnerabilities if not handled properly.

While the xApps in the Near-RT RIC initiate the RIC subscription procedure with the E2 nodes, the subscription manager in the Near-RT RIC platform, enforces the subscription policies and keeps track of the subscriptions initiated by the xApps and the RAN functions, and event triggers associated with those subscriptions. The subscription manager can resolve signaling conflicts among the xApps by one or more of the following means:

- The subscription manager will not allow more than one xApp to subscribe to the same NF based on the same event trigger.
- If more than one xApp subscribes to the same NF and gets the same indication messages from the E2 node, then the subscription manager can allow them to simultaneously control the NF of the E2 node, as long as they do not optimize the same or closely inter-dependent parameters pertaining to the NF.
- If more than one xApp subscribes to the same NF and gets the same indication messages from the E2 node and if they optimize closely inter-dependent parameters, then the subscription manager can allow them to simultaneously control and optimize those parameters by using locks and backoff timers to retain mutual exclusivity.

Authentication aspects of xAPP is explained in § 4.2

5.1.3 User identification inside the Near-RT RIC

Maintaining privacy of the users is of utmost importance inside the RIC. ORAN WG3 is working on the UE identification inside the Near-RT RIC that can be addressed by a combination of 3GPP-defined Trace ID, 3GPP-defined RAN UE ID, temporary RAN network interface-specific UE IDs, and by correlating these IEs with one another. Typically, it is ideal for the Near-RT RIC to maintain persistence of UE identification for near-RT granularities, ranging from 10 ms to 1 s. The xApps are not exposed to UE permanent ID. Invalidation of the temporary IDs in the RIC when they are released in RAN nodes will be handled via normal E2 communication. In neither case is this a UE privacy issue or a DoS attack threat.

5.2 Security aspects of Non-Real-Time Radio Intelligent Controller (Non-RT RIC)

The Non-RT RIC is a component in an O-RAN system for non-real-time control of the RAN through declarative policies and objective intents. This is illustrated in **Figure 6** below.

1. The Non-RT RIC is deployed in a service management and orchestration framework (SMO) and provides declarative policy guidance for cell-level optimization by providing the optimal configuration values for cell parameters over the O1 interface.
2. The Non-RT RIC also sends declarative policies for UE-level optimization to the Near-RT RIC via the A1 interface.
3. The Near-RT RIC then translates the recommended declarative policy from the Non-RT RIC over A1 interface into per-UE control and imperative policy over the E2 interface.
4. The Non-RT RIC develops ML/AI-driven models for policy guidance and non-RT optimization as rApp microservices. These rApps interface with the xApps over the A1 interface to optimize a set of procedures and functions in the underlying RAN.

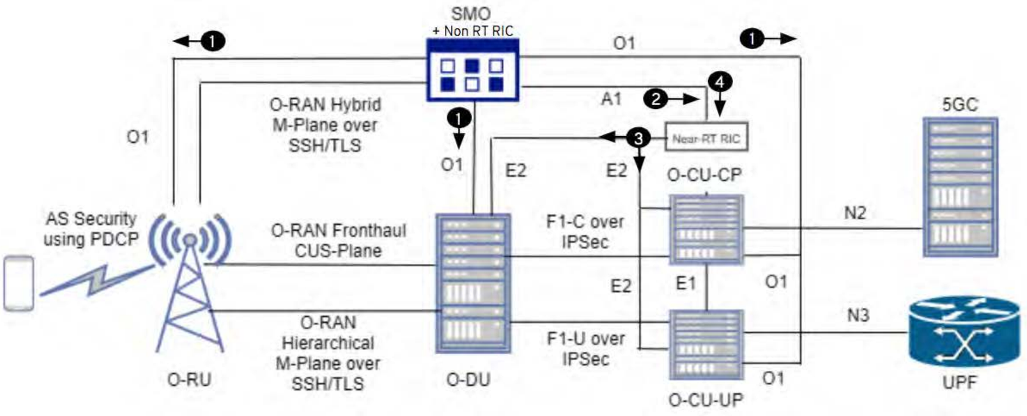
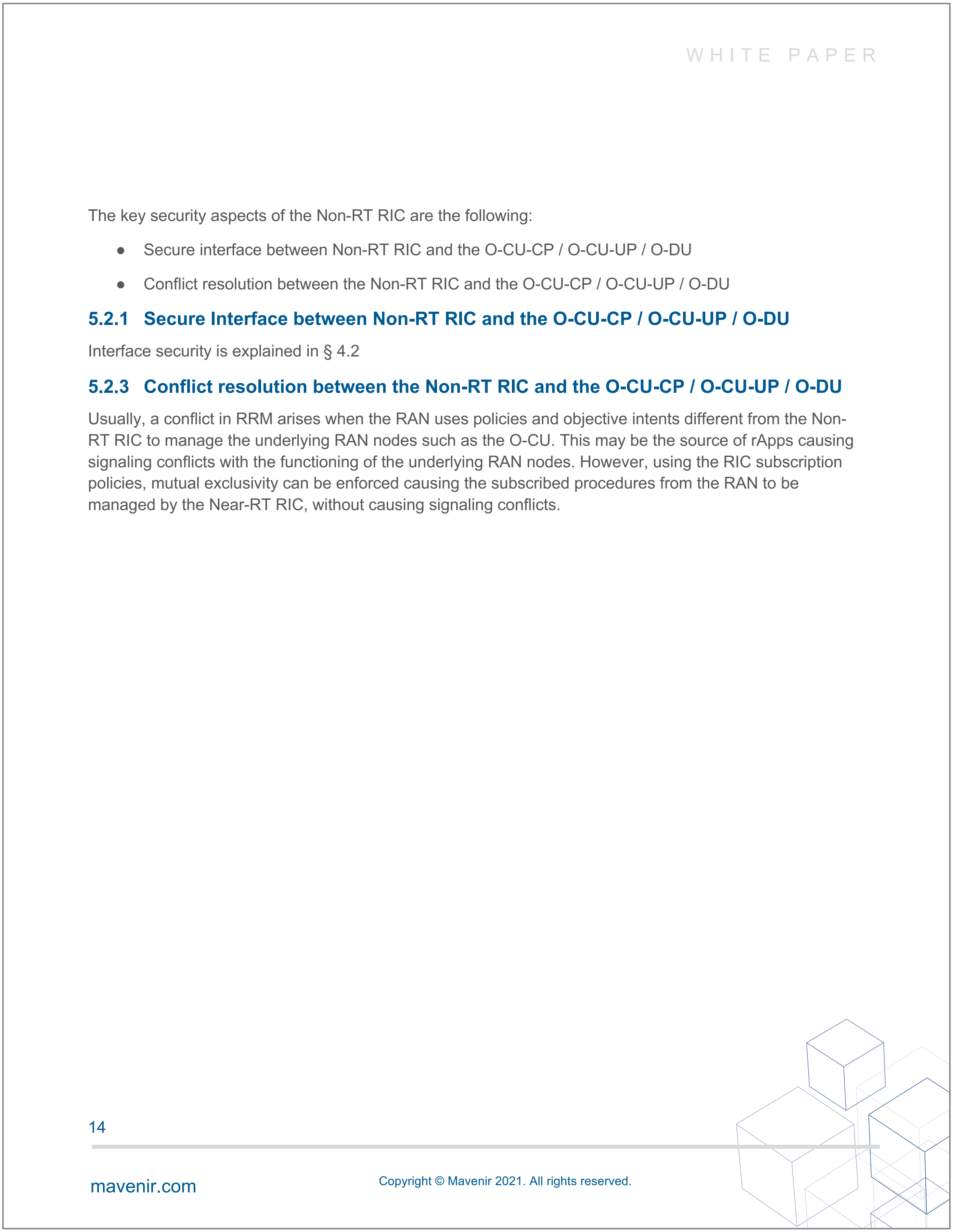


Figure 6: Non-Real-Time RIC declarative policies and objective intents



The key security aspects of the Non-RT RIC are the following:

- Secure interface between Non-RT RIC and the O-CU-CP / O-CU-UP / O-DU
- Conflict resolution between the Non-RT RIC and the O-CU-CP / O-CU-UP / O-DU

5.2.1 Secure Interface between Non-RT RIC and the O-CU-CP / O-CU-UP / O-DU

Interface security is explained in § 4.2

5.2.3 Conflict resolution between the Non-RT RIC and the O-CU-CP / O-CU-UP / O-DU

Usually, a conflict in RRM arises when the RAN uses policies and objective intents different from the Non-RT RIC to manage the underlying RAN nodes such as the O-CU. This may be the source of rApps causing signaling conflicts with the functioning of the underlying RAN nodes. However, using the RIC subscription policies, mutual exclusivity can be enforced causing the subscribed procedures from the RAN to be managed by the Near-RT RIC, without causing signaling conflicts.

6. Secure platform for Network Elements

O-RAN Alliance RAN architecture is built on a fully cloud native architecture – the same cloud architecture that is the bedrock of today's internet and public cloud. The cloud native network functions in the O-RAN network viz. O-CU-CP, O-CU-UP, O-DU, Near-RT RIC and Non-RT RIC, are hosted on a cloud native platform, very similar to the cloud native platform used in the cloud computing industry. The O-RU is a PNF and thus hosted on a non-virtualized platform.

In the following sections we take a holistic look at security aspects of these platforms.

6.1 Secure platform for cloud native network functions

The O-RAN architecture uses a cloud-native platform to host O-CU-CP, O-CU-UP, O-DU, Near-RT RIC and Non-RIT RIC network functions. **Figure 6** shows a typical cloud native platform with three distinct layers:

1. Container-based application software
2. Cloud native software stack comprising an immutable OS, Kubernetes and Container runtime
3. Cloud native hardware infrastructure

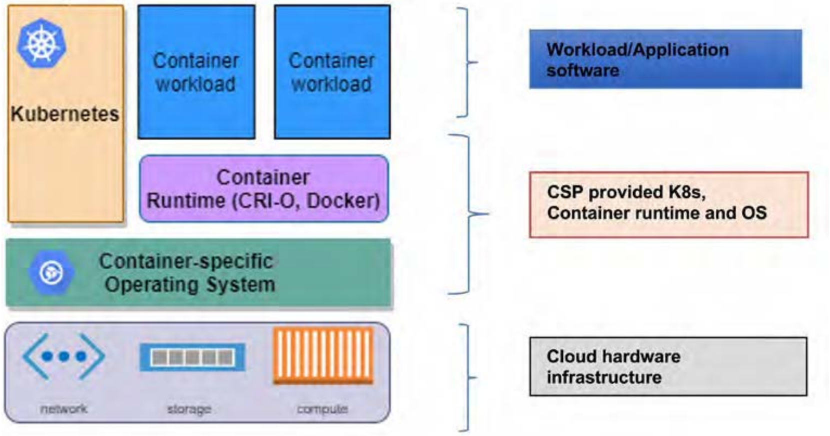

Kubernetes
Container workload
Container workload
Container Runtime (CRI-O, Docker)
Container-specific Operating System
network
storage
compute
Workload/Application software
CSP provided K8s, Container runtime and OS
Cloud hardware infrastructure

Figure 7: Cloud native platform

The following sections look at security features of each of the three layers that make up a cloud native platform.

6.1.1 Security of a container-based application software

A workload is an application or a service deployed on the cloud. Containers offer a packaging infrastructure in which applications and dependent libraries are abstracted from the environment in which they actually run.

Containers are generally perceived to offer less security than virtual machines. But it's worth noting that containers have been in use in the IT industry to build applications such as for banking which are no less critical than telecom applications in terms of security requirements, and the industry has evolved itself in automating its security and establishing best practices.

The following industry standard practices are used in Open RAN to ensure security of the container-based application software:

a) Secure software development based on "secure by design" principles

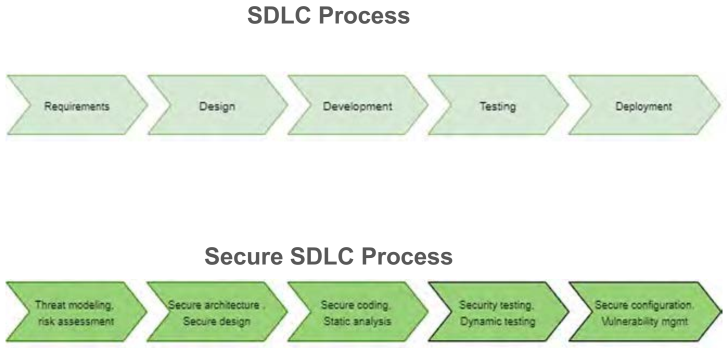
b) Automating security testing based on DevSecOps

c) Vulnerability management in Open Source and 3rd party libraries

Secure software development based on "secure by design" principles

A software development life cycle (SDLC) is a framework for the process of building an application from inception to decommission. In the past, organizations usually performed security-related activities only as part of testing—at the end of the SDLC. As a result of this late-in-the-game technique, they wouldn't find bugs, flaws, and other vulnerabilities until they were far more expensive and time-consuming to fix. Worse yet, they wouldn't find any security vulnerabilities at all.

A secure SDLC involves integrating security testing and other security-related activities into an existing development process. **Figure 7** shows how a standard SDLC process is augmented with security practices at every stage of software development.



SDLC Process

Secure SDLC Process

Requirements
Design
Development
Testing
Deployment
Threat modeling, risk assessment
Secure architecture , Secure design
Secure coding, Static analysis
Security testing, Dynamic testing
Secure configuration, Vulnerability mgmt

Figure 8: Security built into all phases of a software development process

Using a secure SDLC process for the workloads deployed in a O-RAN network such as xAPPs in Near-RT RIC, O-CU-CP and O-CU-UP and O-DU microservices, ensures early detection of flaws in the system, awareness of security considerations by all stakeholders involved in designing, development, testing and deployment of containers, and overall reduction of intrinsic business risks for the organization.

Automating security testing based on DevSecOps

Since the beginning of modern computing, security testing has largely been an independent activity from software development. Security focused QA professionals performed testing during the testing phase.

A DevSecOps approach to the container development lifecycle ensures that security is built-in at every stage of the CI/CD pipeline.

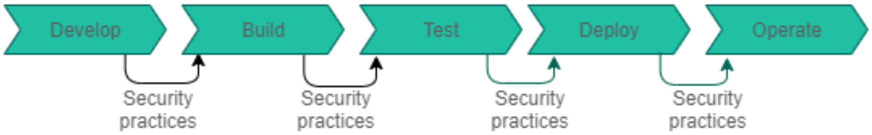


Figure 9: Automated security practices based on DevSecOps

The philosophy behind DevSecOps is to begin security testing early in the SDLC. DevSecOps integrates various security controls into the DevOps workflow such as secure coding analysis using static application security testing (SAST), automated unit, functional and integration testing. This enables developers to fix security issues in their code in near real time rather than waiting until the end of the SDLC.

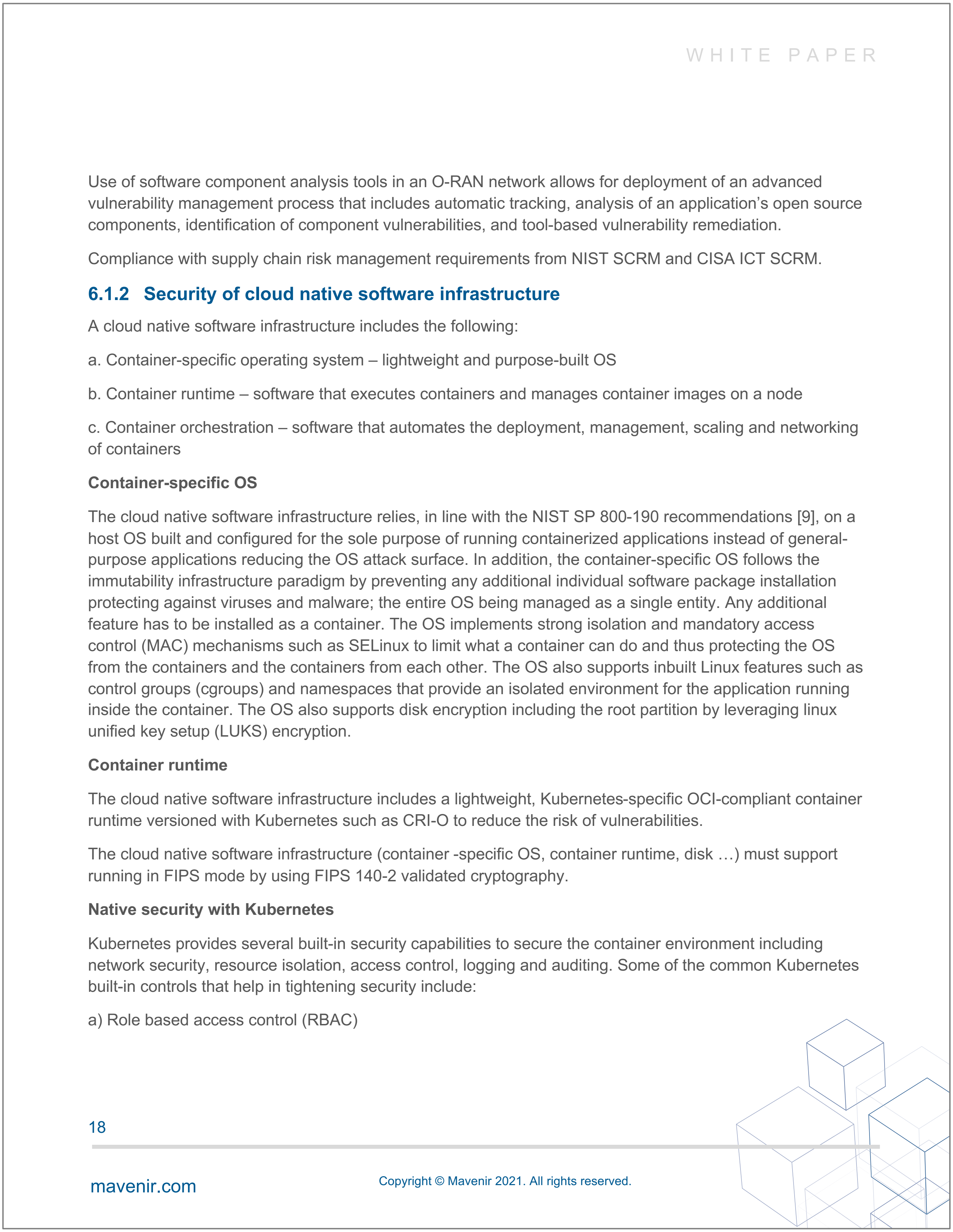
O-RAN Alliance architecture software takes advantage of the advancements in ‘security automation’ and trend in cloud computing towards “shift left.” This ensures that workloads run in the O-RAN network are validated securely (during build/deployment phase) and risk-based timely actions are taken when vulnerabilities are found before they are deployed in operator network.

Vulnerability management of open source and 3rd party libraries

Open source libraries and open source software enable developers to meet the demands of today’s accelerated development timelines. However, they can also open up the platform to attacks due to unaddressed vulnerabilities in the software.

Software component analysis (SCA) is an open source management tool that helps in identifying potential areas of risk from the use of third-party and open-source software. SCA software automatically scans all open-source components, creates an accurate bill of materials (BOM), checks for policy and license compliance, security risks, and version updates. SCA software also provides insights for remedying identified vulnerabilities, usually within the reports generated after a scan.

Specialized container image scanning tools provide automated vulnerability management for containers by identifying and providing remediation paths for all the vulnerabilities in the image. These tools are integrated into the CI/CD pipeline and provide continuous assessment of the container image.



Use of software component analysis tools in an O-RAN network allows for deployment of an advanced vulnerability management process that includes automatic tracking, analysis of an application's open source components, identification of component vulnerabilities, and tool-based vulnerability remediation.

Compliance with supply chain risk management requirements from NIST SCRM and CISA ICT SCRM.

6.1.2 Security of cloud native software infrastructure

A cloud native software infrastructure includes the following:

a. Container-specific operating system – lightweight and purpose-built OS

b. Container runtime – software that executes containers and manages container images on a node

c. Container orchestration – software that automates the deployment, management, scaling and networking of containers

Container-specific OS

The cloud native software infrastructure relies, in line with the NIST SP 800-190 recommendations [9], on a host OS built and configured for the sole purpose of running containerized applications instead of general-purpose applications reducing the OS attack surface. In addition, the container-specific OS follows the immutability infrastructure paradigm by preventing any additional individual software package installation protecting against viruses and malware; the entire OS being managed as a single entity. Any additional feature has to be installed as a container. The OS implements strong isolation and mandatory access control (MAC) mechanisms such as SELinux to limit what a container can do and thus protecting the OS from the containers and the containers from each other. The OS also supports inbuilt Linux features such as control groups (cgroups) and namespaces that provide an isolated environment for the application running inside the container. The OS also supports disk encryption including the root partition by leveraging linux unified key setup (LUKS) encryption.

Container runtime

The cloud native software infrastructure includes a lightweight, Kubernetes-specific OCI-compliant container runtime versioned with Kubernetes such as CRI-O to reduce the risk of vulnerabilities.

The cloud native software infrastructure (container -specific OS, container runtime, disk …) must support running in FIPS mode by using FIPS 140-2 validated cryptography.

Native security with Kubernetes

Kubernetes provides several built-in security capabilities to secure the container environment including network security, resource isolation, access control, logging and auditing. Some of the common Kubernetes built-in controls that help in tightening security include:

a) Role based access control (RBAC)

Use of RBAC in the cluster provides a framework for implementing the principle of least privilege for humans and applications accessing the Kubernetes API.

b) Configure the security context for pods to limit their capabilities

Pod security policy sets defaults for how workloads are allowed to run in the cluster. These controls can eliminate entire classes of attacks that depend on privileged access.

c) Use Kubernetes network policies to control traffic between pods and clusters.

Kubernetes' network policies allow control of network access into and out of the containerized applications. In addition to this feature, software-based firewalls may be deployed to control container to container communication within or across different clusters.

d) Use namespaces to isolate sensitive workloads and create security boundaries – separating workloads into namespaces can help contain attacks and limit the impact of mistakes or destructive actions by authorized users.

e) Assess the container privileges – Adhering to the principle of least privilege and provide the minimum privileges and capabilities that would allow the container to perform its intended function.

f) Use mutual Transport Layer Security (TLS) for all inter cluster and intra cluster communications.

g) Capability to encrypt the etcd datastore to protect infrastructure and application secrets or to support integration with external vaults.

Leveraging Kubernetes operators for security

Kubernetes operators are software extensions to Kubernetes that make use of custom resources to manage services and their components in an automated way. These operators can be leveraged by the cloud native software platform for specific security purposes:

- Hardware management operators to restrict the need for applications of elevated privileges
- Compliance operators to continuously monitor the compliance of the cluster
- File integrity monitoring operators to detect any attacks impacting the platform integrity
- Platform management operators to fight configuration drift and enforce a secure configuration by eliminating human errors
- Audit and log operators to manage the audit configuration and the log forwarding to a SIEM

A cloud native-based O-RAN network can leverage native security controls in container runtime and container orchestration platforms such as Kubernetes, to provide defense in depth security for the containerized workload that they host.

Secure configuration of the cloud infrastructure based on industry benchmarks

The cloud infrastructure is configured based on industry best practices such as CIS benchmarks for operating system, Docker and Kubernetes, and Network Equipment Security Assurance Scheme (NESAS) jointly defined by 3GPP and GSMA provides a consistent framework and common external audit program for multiple vendors and operators. This ensures that appropriate security controls are put-in-place in the platform, thus reducing its attack surface.

Some of the common security controls include disabling unused ports and unused service, principle of least privileges (PLoP) for workloads, protecting data in storage, user access control using RBAC, etc.

All virtualized platforms in an O-RAN network are hardened as per 3GPP's security assurance specifications [10] and other well-known industry benchmarks such as those from CIS [11]. This ensures that security controls are implemented at every layer of the platform thus reducing the platform's attack surface.

Detecting and remediating configuration errors with cloud security posture management

Misconfiguration is the #1 cause of cloud-based data breaches. A mechanism is needed to make sure the configuration of the deployed cloud resources is correct and secure on day one, and that they stay that way on day two and beyond. This is referred to as cloud security posture management (CSPM).

The cloud industry has used CSPM security tools to continuously monitor cloud environments for detection of cloud misconfiguration vulnerabilities that can lead to compliance violations and data breaches.

With the adoption of a cloud native architecture in O-RAN based networks, an operator now has the means to deploy advanced CSPM tools to guard against natural “drift” of on network configuration and reduce the potential for attacks.

Commercial cloud native hybrid platform

Standardizing on a commercial cloud native hybrid platform enables the operator with the following security benefits:

- A Kubernetes-certified platform with the flexibility to run securely on-prem or in a virtual private cloud, supporting O-RAN topology variations from the SMO, RICs, CUs, and DUs with zero-touch provisioning,
- Extended software lifecycle with dynamic updates that address new CVEs and optimizations over time into disconnected environments,
- Support for multi-tenancy so that multi-vendor software can be securely hosted in the same cluster,
- Support for infrastructure compliance scanning (OpenSCAP) and remediation,
- A container registry with vulnerability scanning to eliminate vulnerabilities on O-RAN platforms (e.g Near Real-Time RIC) and associated xApps and rApps.

6.1.3 Security considerations with a cloud native hardware infrastructure

O-RAN enables decoupling of hardware and software, allowing for a platform to be built from different vendors.

6.1.3.1 Secure storage of credentials and data at rest

It is recommended that O-RAN hardware comes with a hardware-based security module like TPM to manage, generate, and securely store cryptographic keys. Hardware-based security modules are also

meant to provide a hardware root of trust to enable secure computing by providing a secure key storage enclave with minimal cryptographic functions primarily in the signing and signature verification space.

The data at rest must be encrypted using keys generated from hardware-based security modules.

6.1.3.2 Establishing software chain of trust

Zero-trust cannot be achieved without the full participation of all the elements in the trust chain for a network. **Figure 9** illustrates key aspects of establishing chain of trust when adhering to zero-trust in digital systems.

Trusted hardware

The hardware is built with a tamper resistant "hardware root of trust" device that provides a secure environment for storing cryptographic keys and for attestation of certificates and all the software running on that hardware. The device will expose a simple user interface for the application to use when it needs to use the device for storing keys, retrieving certificates etc.

Trusted software

Software signing is enforced at all software layers including the firmware, cloud native software stack and container workloads at time of deployment, as well as authenticated version upgrades to make it more difficult to introduce malicious software into operator-controlled elements.

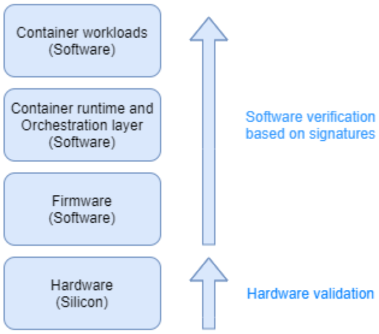

Container workloads (Software)
Container runtime and Orchestration layer (Software)
Firmware (Software)
Hardware (Silicon)
Software verification based on signatures
Hardware validation

Figure 10 Secure boot using a hardware root of trust

Establishing end-to-end chain of trust with secure boot

Secure boot requires that every boot up is starting from a piece of software that cannot be updated in the field. This piece of software is referred to as Core Root of Trust for Measurement (CRTM).

Thereafter, during the boot process every software program in the platform will be integrity verified before its execution by the software at the lower layer. This establishes an end-to-end software chain of trust. The trust anchor for the software integrity verification is software signing certificate.

In the O-RAN network, it is recommended to use secure boot based on hardware root of trust and software signing to establish an end-to-end chain of trust.

6.2 Secure platform for O-RU

An attacker with unauthorized access to the management interface of an unprotected O-RU could allow an attacker to steal unprotected private keys, certificates, hash values and/or inject malwares and/or manipulate existing O-RU software. An attacker could further launch denial-of-service, intrusion, and replay attacks on other network elements including an O-DU.

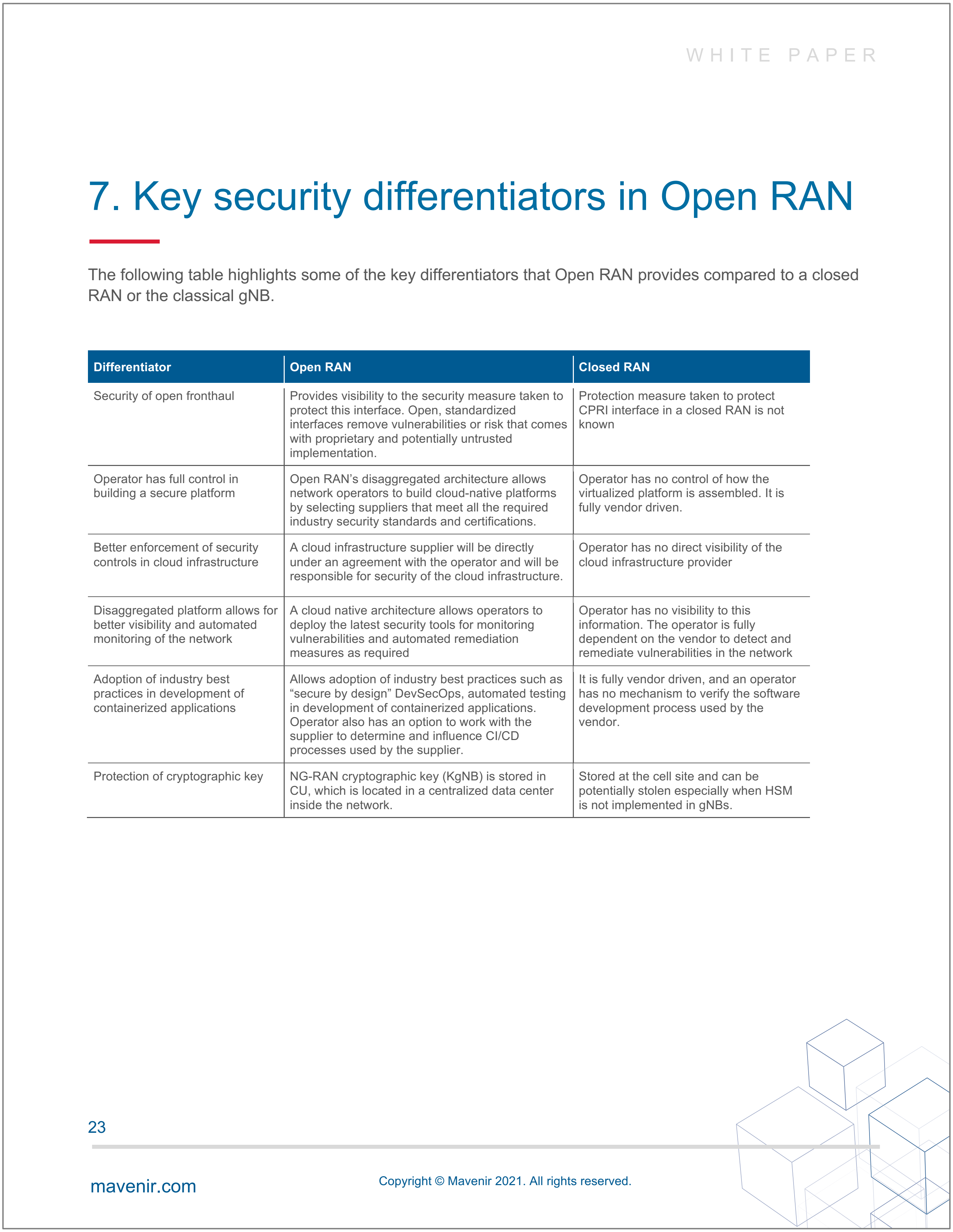
Therefore, hardening of the O-RU platform will ensure enough equipment security to substantially reduce the attack surface that would otherwise exist in an unprotected O-RU. Security precautions on the O-RU can be divided into three aspects.

1. Supply chain security
2. Physical security
3. Network security

Supply chain security ensures that throughout the supply chain process of manufacturing, from O-RU to its final installation site and commissioning, a controlled secure chain of custody process is followed. This ensures that the O-RU is properly tracked and tagged.

Physical security ensures that the physical O-RU is sealed with non-tamper-able screws that cannot be easily broken or opened and in the event of tampering or forced opening, all O-RU functionality will be disabled so that the O-RU becomes inoperable. This is in addition to all the physical and logical ports being secured and isolated, so that they cannot be used as a vulnerability entrance into the extended RAN network.

From a network security point of view, O-RU ensures that all authentication and communication security protocols are correctly performed and followed. To ensure reliable and secure software upgrades, the TPM procedures are implemented so that rogue software downloads are prevented. Finally, hardening features, such as disabling unnecessary software components and interfaces when not in use, running software at the correct privilege-level, scrambling/encryption of data in storage, and secure boot and hardware-based security module, are part of the comprehensive security processes on the typical O-RU to ward off as well as prevent unauthorized access to the O-RU.



7. Key security differentiators in Open RAN

The following table highlights some of the key differentiators that Open RAN provides compared to a closed RAN or the classical gNB.

Differentiator	Open RAN	Closed RAN
Security of open fronthaul	Provides visibility to the security measure taken to protect this interface. Open, standardized interfaces remove vulnerabilities or risk that comes with proprietary and potentially untrusted implementation.	Protection measure taken to protect CPRI interface in a closed RAN is not known
Operator has full control in building a secure platform	Open RAN's disaggregated architecture allows network operators to build cloud-native platforms by selecting suppliers that meet all the required industry security standards and certifications.	Operator has no control of how the virtualized platform is assembled. It is fully vendor driven.
Better enforcement of security controls in cloud infrastructure	A cloud infrastructure supplier will be directly under an agreement with the operator and will be responsible for security of the cloud infrastructure.	Operator has no direct visibility of the cloud infrastructure provider
Disaggregated platform allows for better visibility and automated monitoring of the network	A cloud native architecture allows operators to deploy the latest security tools for monitoring vulnerabilities and automated remediation measures as required	Operator has no visibility to this information. The operator is fully dependent on the vendor to detect and remediate vulnerabilities in the network
Adoption of industry best practices in development of containerized applications	Allows adoption of industry best practices such as "secure by design" DevSecOps, automated testing in development of containerized applications. Operator also has an option to work with the supplier to determine and influence CI/CD processes used by the supplier.	It is fully vendor driven, and an operator has no mechanism to verify the software development process used by the vendor.
Protection of cryptographic key	NG-RAN cryptographic key (KgNB) is stored in CU, which is located in a centralized data center inside the network.	Stored at the cell site and can be potentially stolen especially when HSM is not implemented in gNBs.

8. Conclusion

At the heart of Open RAN is the use of cloud native architecture, the same architecture that is the bedrock of today's internet and public cloud. Security practices in virtualized deployments are mature and used across the cloud computing industry. Virtualized deployment in telecom networks is not new. Operators already have virtualized infrastructure in their data centers and many have deployed virtual workloads for other components in the network including: packet core, IMS, and other applications such as CDN. With a disaggregated architecture, operators will now additionally benefit from security expertise and experience of today's large cloud infrastructure suppliers in managing the security of large IT cloud environments.

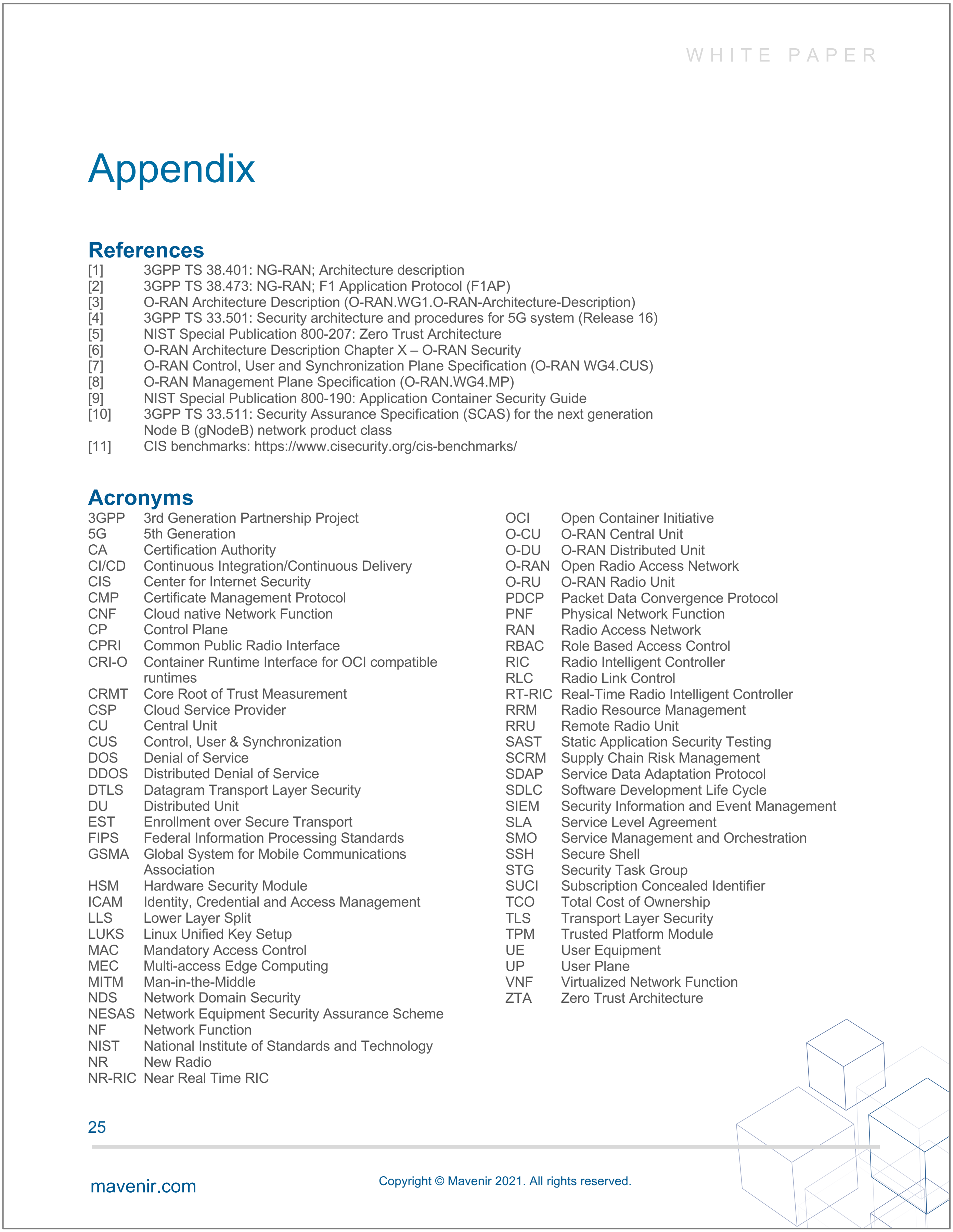
Operator regains control as the operator now understands what is required to build and maintain a secure infrastructure. Open RAN is built on a cloud native platform with clear responsibilities and accountability established between hardware/infrastructure suppliers, a hybrid-cloud platform supplier, and RAN software suppliers. It enables network operators to select suppliers that meet all the required industry security standards and certifications.

Open RAN leverages several security industry best practices used in the cloud computing industry. A "shift-left" strategy in the software development process integrates security controls and practices into every phase of the software development. With DevSecOps integrated into the CI/CD pipeline, this also brings automation into secure code reviews and security testing. Use of automated tools for detection, remediation of vulnerabilities in open-source software and detection, and management of secure posture provides an operator with quick detection and resolution of anomalies in the network.

O-RAN Alliance's architecture for RAN is built on the secure foundation of zero trust where network elements mutually authenticate with each other in order to communicate. All communication between them is transported over a secure interface per industry best practices specified by O-RAN Alliance's security specifications. While standards are still evolving, the Open RAN pioneers and ecosystem vendors like Altiostar, Mavenir, Fujitsu and Red Hat, as well as early adopters like Rakuten, Vodafone, Telefonica, NTT Docomo and DISH have ensured that all the interfaces are secured using certificate based security.

Every network element in the Open RAN network undergoes platform hardening as per 3GPP's security assurance specifications and other well-known cloud computing industry benchmarks such as CIS. This protects the network from an attacker gaining unauthorized access and subjecting the network to Denial-Of-Service (DOS) attacks or gaining illegal access.

> In summary, open, standardized interfaces remove vulnerabilities or risk that comes with proprietary and potentially untrusted implementation and provides an operator full visibility and control over the cloud environment and network in general.



Appendix

References

[1] 3GPP TS 38.401: NG-RAN; Architecture description

[2] 3GPP TS 38.473: NG-RAN; F1 Application Protocol (F1AP)

[3] O-RAN Architecture Description (O-RAN.WG1.O-RAN-Architecture-Description)

[4] 3GPP TS 33.501: Security architecture and procedures for 5G system (Release 16)

[5] NIST Special Publication 800-207: Zero Trust Architecture

[6] O-RAN Architecture Description Chapter X – O-RAN Security

[7] O-RAN Control, User and Synchronization Plane Specification (O-RAN WG4.CUS)

[8] O-RAN Management Plane Specification (O-RAN.WG4.MP)

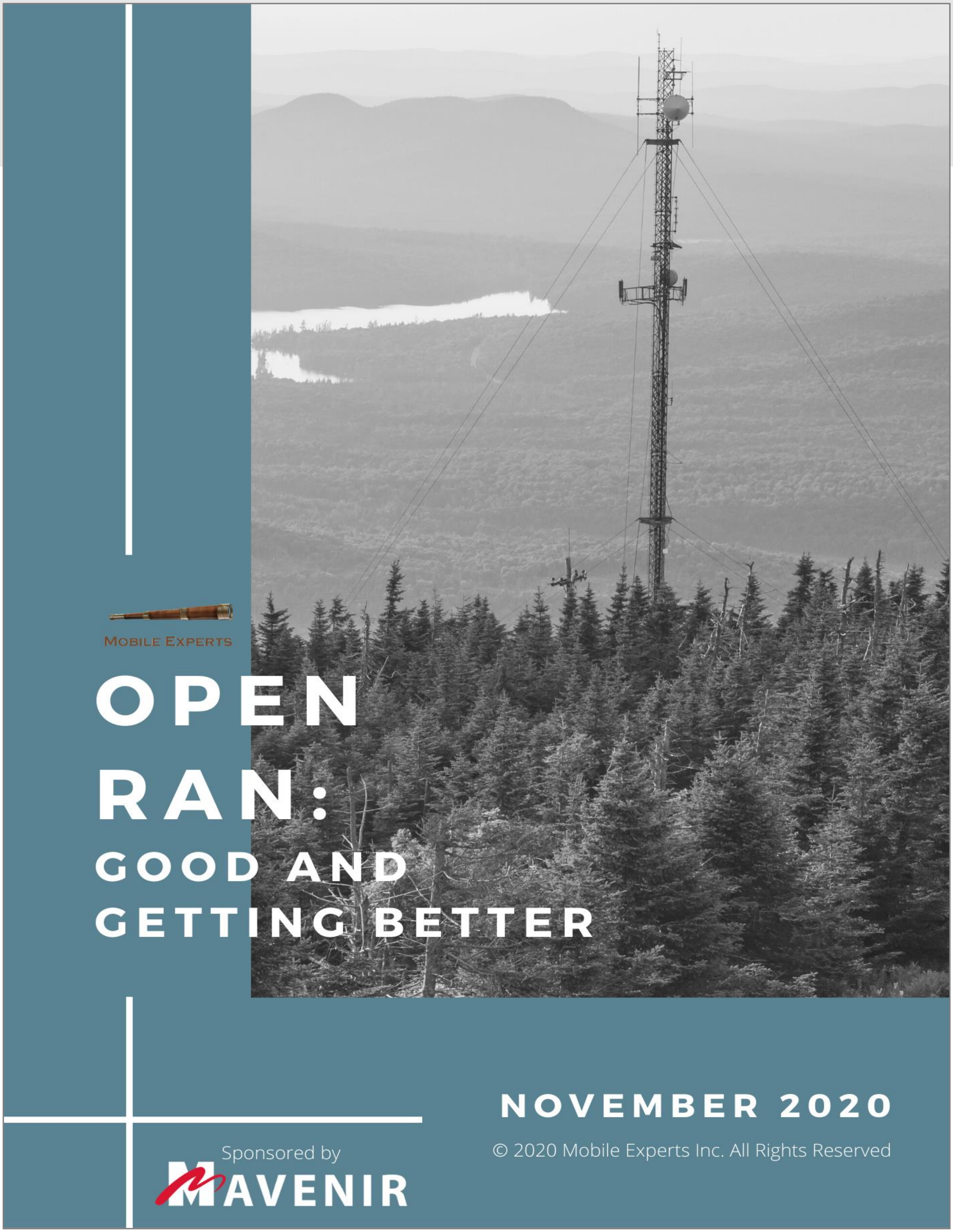
[9] NIST Special Publication 800-190: Application Container Security Guide

[10] 3GPP TS 33.511: Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class

[11] CIS benchmarks: https://www.cisecurity.org/cis-benchmarks/

Acronyms

3GPP	3rd Generation Partnership Project
5G	5th Generation
CA	Certification Authority
CI/CD	Continuous Integration/Continuous Delivery
CIS	Center for Internet Security
CMP	Certificate Management Protocol
CNF	Cloud native Network Function
CP	Control Plane
CPRI	Common Public Radio Interface
CRI-O	Container Runtime Interface for OCI compatible runtimes
CRMT	Core Root of Trust Measurement
CSP	Cloud Service Provider
CU	Central Unit
CUS	Control, User & Synchronization
DOS	Denial of Service
DDOS	Distributed Denial of Service
DTLS	Datagram Transport Layer Security
DU	Distributed Unit
EST	Enrollment over Secure Transport
FIPS	Federal Information Processing Standards
GSMA	Global System for Mobile Communications Association
HSM	Hardware Security Module
ICAM	Identity, Credential and Access Management
LLS	Lower Layer Split
LUKS	Linux Unified Key Setup
MAC	Mandatory Access Control
MEC	Multi-access Edge Computing
MITM	Man-in-the-Middle
NDS	Network Domain Security
NESAS	Network Equipment Security Assurance Scheme
NF	Network Function
NIST	National Institute of Standards and Technology
NR	New Radio
NR-RIC	Near Real Time RIC
OCI	Open Container Initiative
O-CU	O-RAN Central Unit
O-DU	O-RAN Distributed Unit
O-RAN	Open Radio Access Network
O-RU	O-RAN Radio Unit
PDCP	Packet Data Convergence Protocol
PNF	Physical Network Function
RAN	Radio Access Network
RBAC	Role Based Access Control
RIC	Radio Intelligent Controller
RLC	Radio Link Control
RT-RIC	Real-Time Radio Intelligent Controller
RRM	Radio Resource Management
RRU	Remote Radio Unit
SAST	Static Application Security Testing
SCRM	Supply Chain Risk Management
SDAP	Service Data Adaptation Protocol
SDLC	Software Development Life Cycle
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SMO	Service Management and Orchestration
SSH	Secure Shell
STG	Security Task Group
SUCI	Subscription Concealed Identifier
TCO	Total Cost of Ownership
TLS	Transport Layer Security
TPM	Trusted Platform Module
UE	User Equipment
UP	User Plane
VNF	Virtualized Network Function
ZTA	Zero Trust Architecture



MOBILE EXPERTS

OPEN RAN:

GOOD AND GETTING BETTER

NOVEMBER 2020

Sponsored by MAVENIR

Open RAN: Good and getting better

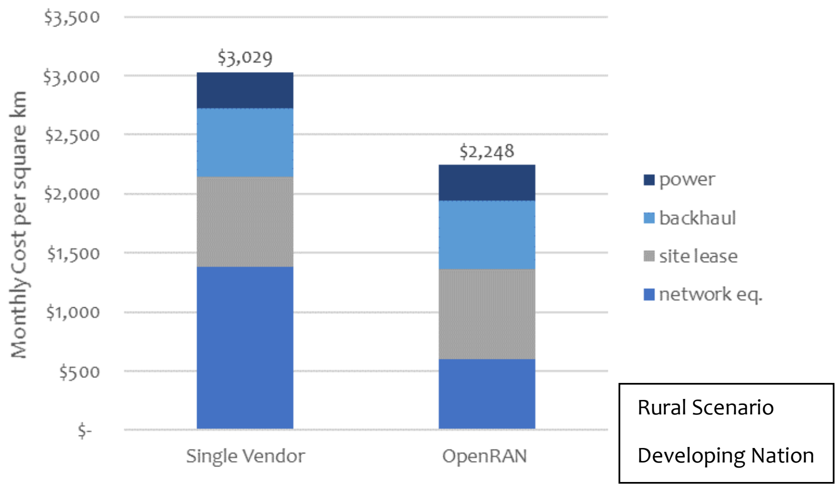
November 2020

Open RAN interfaces have become an important part of building 5G mobile networks. And it's not just the greenfield networks and third-world networks that will benefit. This white paper provides some details on how Open RAN standards will impact almost every 5G network over the next five years.

Where ORAN Stands Today

In addition to the greenfield networks that have embraced OpenRAN (Rakuten/Dish) Vodafone, Vodafone Idea, Reliance Jio, Telefonica, MTN, and other operators have also committed to deployment using Open RAN standards to realize cost savings, and future proof their networks, and to add flexibility for vendor mixing (widening the supply chain) . The trials conducted by these major players so far indicate that the technology has reached a level of maturity ***that is ready*** for commercial networks. The best example is Rakuten in Japan, who has deployed more than 5,000 'radio stations' so far and has already upgraded its network from 4G to 5G, using a collection of at least 18 vendors providing individual components of the network. Rakuten was able to sign up more than a million subscribers in its first three months.

Greenfield and multi-national operators are keen to use Open RAN standards because they see significant cost savings. In a greenfield deployment scenario, we calculate that the Total Cost of Ownership can be roughly 26% lower for an Open RAN network, based on more competitive pricing on radio equipment, maintenance contracts, and software.

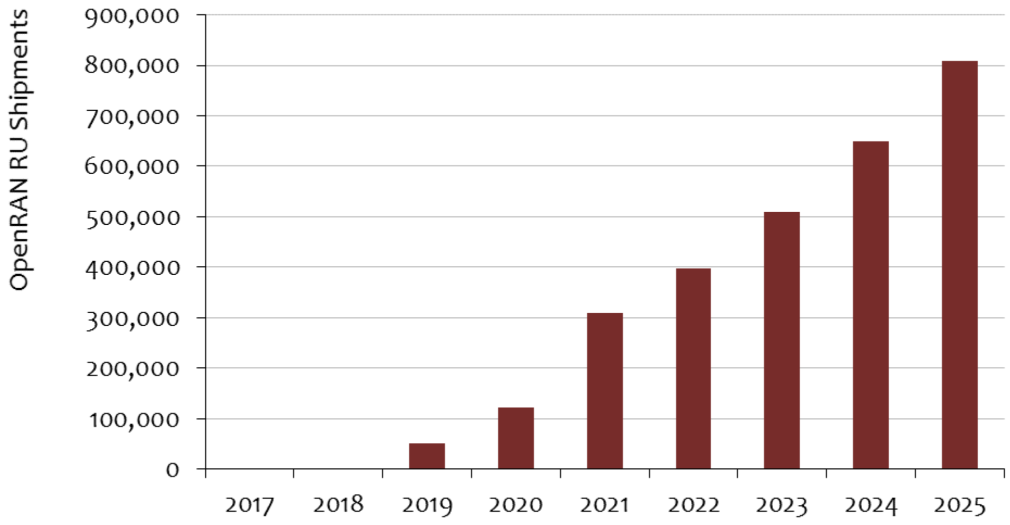


Rural Scenario

Developing Nation

Because of this kind of cost savings, Mobile Experts predicts that the market will move decisively to use the OpenRAN 'mix and match' approach. The number of OpenRAN-based

RUs deployed by operators and private networks will grow to more than 800,000 Radio Units in 2025, from only 122,000 in 2020.



Challenges for OpenRAN

So far, the OpenRAN story has a happy ending, ramping up to more than 10% of the market in the first few years. But as the story goes on, there are some challenges. The latest release of O-RAN Alliance standards in April 2020 set up interoperability for all of the main functionality of 3GPP standards, but O-RAN specifications do not cover some areas where 3GPP has neglected to standardize operation between different vendors, such as:

- Carrier Aggregation,
- Coordinated MultiPoint (CoMP),
- enhanced Inter-cell Interference Coordination (eICIC), and
- PIM Cancellation.

These features are not critical in greenfield and rural networks, so they don't really affect the initial adoption of Open RAN in the initial market areas. However, these features become important when openness is applied to high-density urban networks. That's where interference levels begin to limit the network, and efficient use of spectrum becomes a key metric for the business case.

High-density urban networks are complicated because big cities already have multiple bands of LTE service today. Adding an OpenRAN 5G network on top of a multi-band LTE network will be difficult to optimize between vendors without coordination at a very detailed level…it's not as simple as simply plugging in 5G on a new band. It's important to coordinate so that the operator can get the benefits of CA, EN-DC, and PIM cancellation across multiple bands and modes.

Another challenge is for OpenRAN-based small cells to coexist with an incumbent vendor's macro network on the same frequency band. Out of thirty mobile operators interviewed, ALL of them expect to use the O-RAN Alliance specifications to require interoperability in future macro networks, even where they don't expect to buy RUs and DUs from different vendors. The reason for this: the operators want the flexibility to add a third-party RU in the future, either for an in-building application, or an outdoor hotspot, or a special case like a tunnel. OpenRAN with a single network architecture offers this capability, and in fact Mavenir has demonstrated connectivity for specialized tunnel radios already.

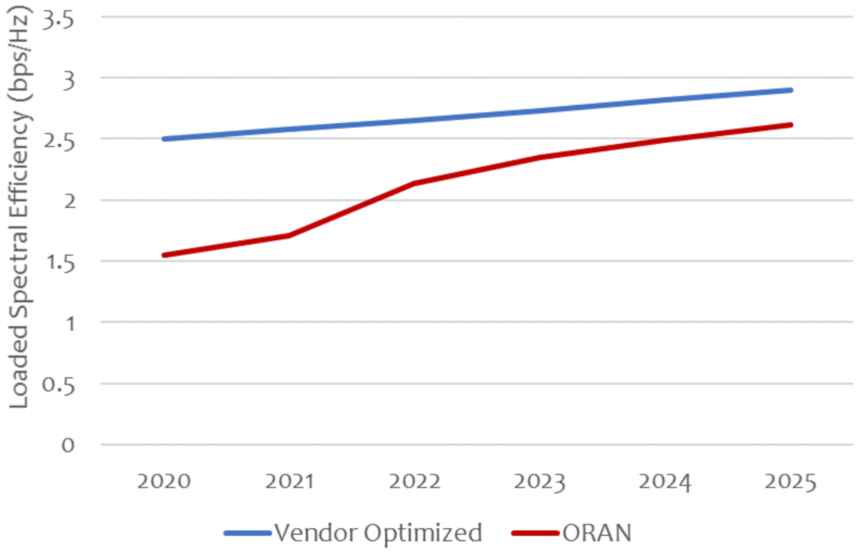
In order to make OpenRAN work for two vendors on the same band in a hetnet scenario, the operators will need much deeper coordination of features such as CoMP and Carrier Aggregation. The lack of complete standardization in 3GPP or elsewhere will make this challenge difficult to solve in the traditional RAN committees.

The Industry Can Solve the Challenges and operators need to take control

To deal with the high-capacity challenge, we expect the O-RAN Alliance to continue their development of standards, driving another layer deeper into the technology in order to standardize inter-vendor operation for CA, CoMP, eICIC, and other features. The Alliance may run into resistance from the incumbent OEMs, who rely on these features to differentiate their products, so the operators are likely to use other organizations to apply pressure to the OEMs and bypass any roadblocks. In this way, the Telecom Infra Project (TIP), CPRI Alliance, 3GPP, the Open Networking Foundation (ONF), and other groups may play a role in setting new standards. In particular, ONF has created an SD-RAN project, driven by major players such as AT&T, China Mobile, China Unicom, Deutsche Telekom, NTT, Facebook, and Google, with key participation from other players such as Intel, Mavenir, Radisys, and Sercomm.. As an engineering team, the ONF SD-RAN project is focused on using the RAN Intelligent Controller (RIC) to gain more control over functions within the RAN and use applications with AI/ML to drive performance improvements.

The ONF group is important, as it enables the operators to bypass any obstacles that the incumbent suppliers create. The O-RAN Alliance and ONF groups are a mechanism for operators to take control back from these suppliers ensuring that all interfaces, including those that have been specified by 3GPP are open and are made available free of charge. A good example of this is the X2 interface that is fully specified but kept locked or licensed. Removing these arbitrary license fees will provide further cost reductions and multivendor deployments to roll out more easily in built-out networks.

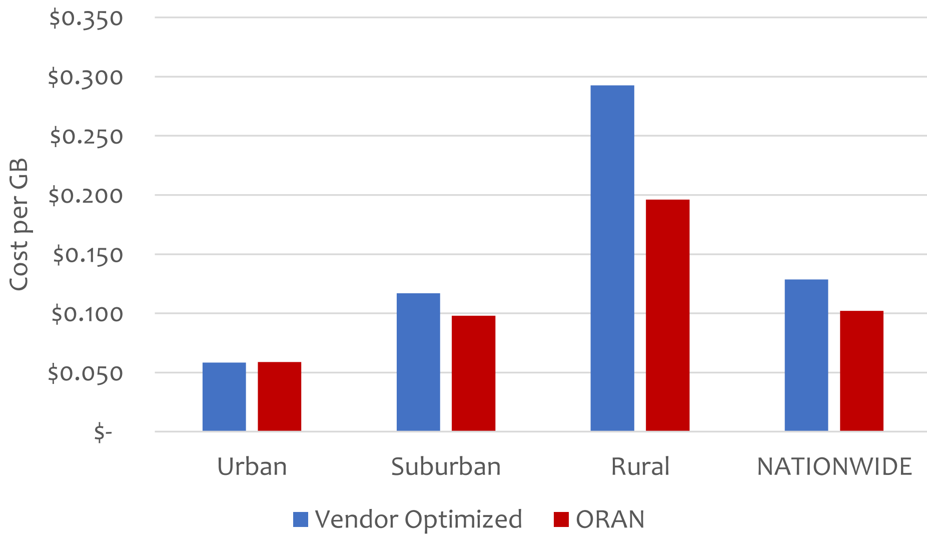
One way or another, we expect the operators to keep pushing to achieve higher performance in open radio networks. In doing so, over a period of 3-4 years they should be able to achieve competitive performance for high-capacity applications as well as greenfield and rural applications.



What will happen in the mid- to long term

The strong operator support behind ONF and O-RAN Alliance appears to be strongly unified and should be effective at driving performance improvements. Coordination between TIP, 3GPP, ONF, and O-RAN Alliance is good, eliminating the destructive confusion that has happened in other standardization efforts. Essentially, the RAN is now on a trajectory that was followed by Ethernet and by passive optical networking over the years, both of which resulted in cost savings through openness. As a result, we believe that it's possible for the ORAN community to approach the loaded spectral efficiency performance of a single-vendor network within the next 4-5 years.

Of course, we all know from experience that performance is not enough. Because the big vendors control the 2G, 3G, and 4G networks in the field today, they will try to continue to control the compatibility of the installed base with new OpenRAN equipment . (Vendors that play hardball too aggressively can and will be replaced, but that's expensive.) In general, operators will need time to transition their legacy networks, by shutting down 2G and 3G and by upgrading 4G networks to 5G.



2025 Scenario

Nationwide

Developed Nation

By 2025, we expect that ORAN will save money in multiple market segments, including both high-capacity applications and coverage-limited applications. When that happens, the OpenRAN business model will be applied to networks ranging from urban to rural in many mainstream markets. As we apply our cost models to this future scenario, we find that the cost of delivering data will be competitive with (reduced) prices from the top OEMs in the urban case, but cost will be significantly lower in the critical suburban and rural segments.

In the end, the industry is on track to drive OpenRAN from its starting point in greenfield networks into the mainstream markets with highly complex urban networks. The future is bright for OpenRAN.

Future Proofing Mobile Network Economics

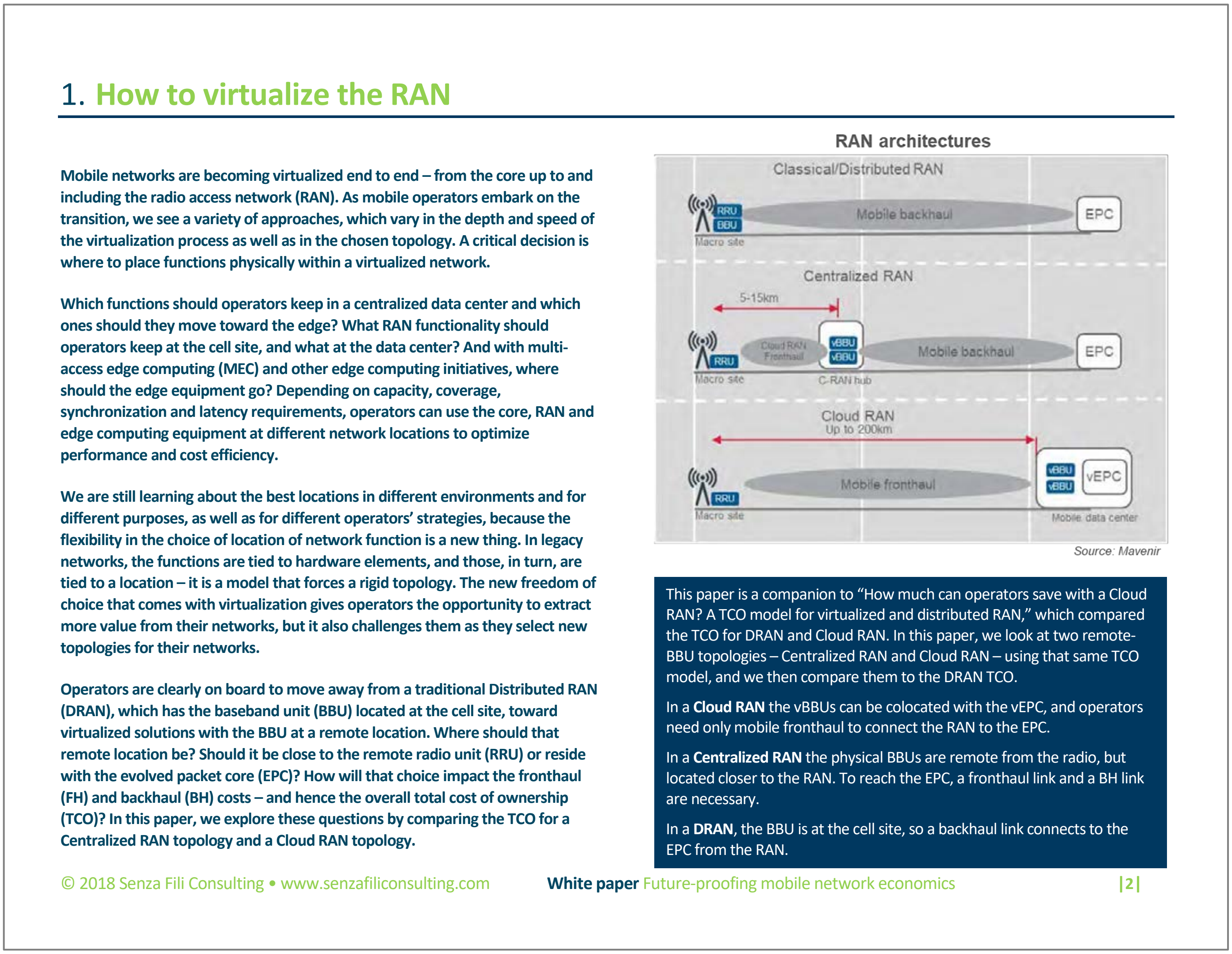
Assessing the TCO for Cloud RAN and Centralized RAN

BY MONICA PAOLINI
SENZA FILI

SENZA FILI

SPONOSORED BY

MAVENIR



1. How to virtualize the RAN

Mobile networks are becoming virtualized end to end – from the core up to and including the radio access network (RAN). As mobile operators embark on the transition, we see a variety of approaches, which vary in the depth and speed of the virtualization process as well as in the chosen topology. A critical decision is where to place functions physically within a virtualized network.

Which functions should operators keep in a centralized data center and which ones should they move toward the edge? What RAN functionality should operators keep at the cell site, and what at the data center? And with multi-access edge computing (MEC) and other edge computing initiatives, where should the edge equipment go? Depending on capacity, coverage, synchronization and latency requirements, operators can use the core, RAN and edge computing equipment at different network locations to optimize performance and cost efficiency.

We are still learning about the best locations in different environments and for different purposes, as well as for different operators' strategies, because the flexibility in the choice of location of network function is a new thing. In legacy networks, the functions are tied to hardware elements, and those, in turn, are tied to a location – it is a model that forces a rigid topology. The new freedom of choice that comes with virtualization gives operators the opportunity to extract more value from their networks, but it also challenges them as they select new topologies for their networks.

Operators are clearly on board to move away from a traditional Distributed RAN (DRAN), which has the baseband unit (BBU) located at the cell site, toward virtualized solutions with the BBU at a remote location. Where should that remote location be? Should it be close to the remote radio unit (RRU) or reside with the evolved packet core (EPC)? How will that choice impact the fronthaul (FH) and backhaul (BH) costs – and hence the overall total cost of ownership (TCO)? In this paper, we explore these questions by comparing the TCO for a Centralized RAN topology and a Cloud RAN topology.

RAN architectures

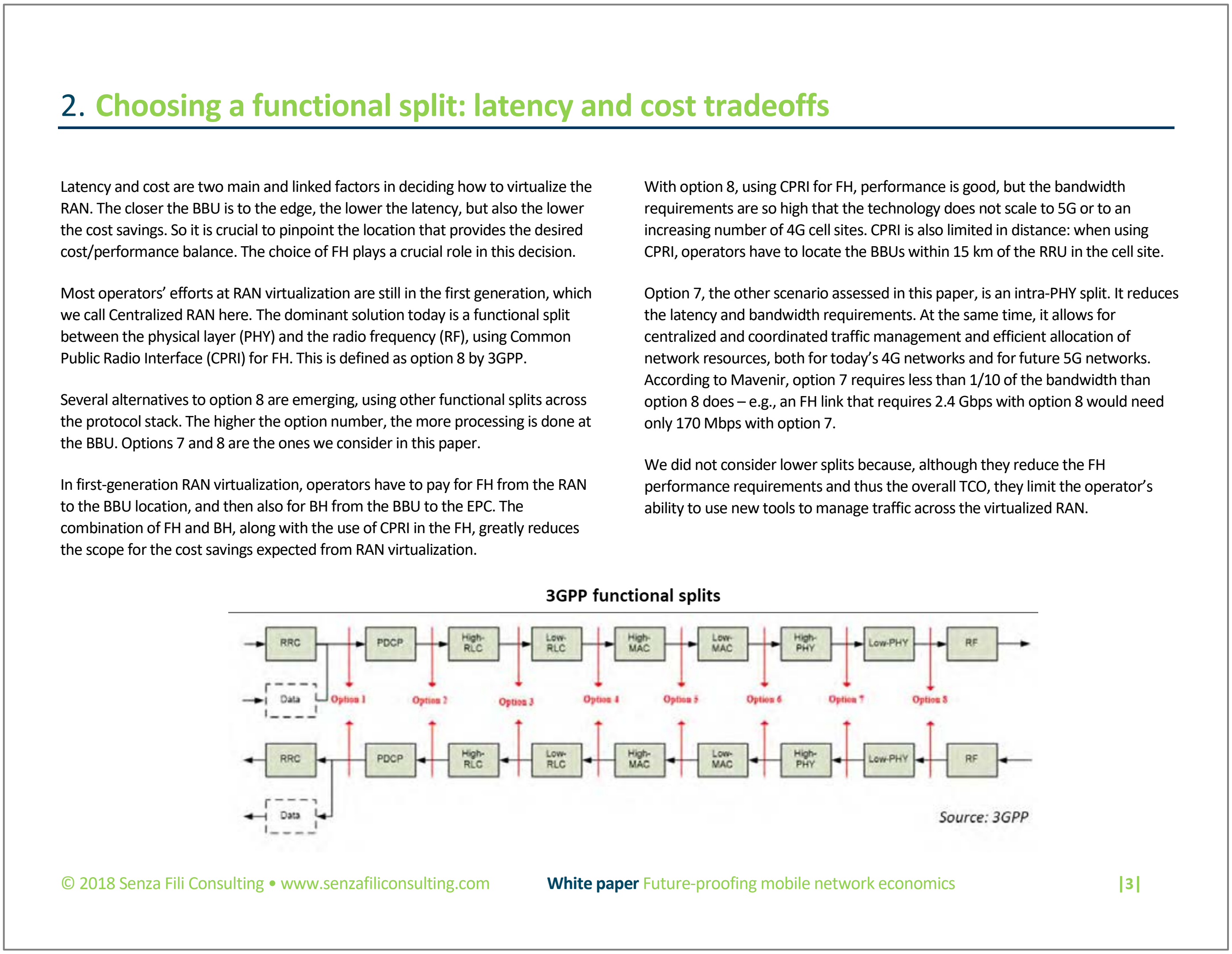
Source: Mavenir

This paper is a companion to "How much can operators save with a Cloud RAN? A TCO model for virtualized and distributed RAN," which compared the TCO for DRAN and Cloud RAN. In this paper, we look at two remote-BBU topologies – Centralized RAN and Cloud RAN – using that same TCO model, and we then compare them to the DRAN TCO.

In a **Cloud RAN** the vBBUs can be colocated with the vEPC, and operators need only mobile fronthaul to connect the RAN to the EPC.

In a **Centralized RAN** the physical BBUs are remote from the radio, but located closer to the RAN. To reach the EPC, a fronthaul link and a BH link are necessary.

In a **DRAN**, the BBU is at the cell site, so a backhaul link connects to the EPC from the RAN.



2. Choosing a functional split: latency and cost tradeoffs

Latency and cost are two main and linked factors in deciding how to virtualize the RAN. The closer the BBU is to the edge, the lower the latency, but also the lower the cost savings. So it is crucial to pinpoint the location that provides the desired cost/performance balance. The choice of FH plays a crucial role in this decision.

Most operators' efforts at RAN virtualization are still in the first generation, which we call Centralized RAN here. The dominant solution today is a functional split between the physical layer (PHY) and the radio frequency (RF), using Common Public Radio Interface (CPRI) for FH. This is defined as option 8 by 3GPP.

Several alternatives to option 8 are emerging, using other functional splits across the protocol stack. The higher the option number, the more processing is done at the BBU. Options 7 and 8 are the ones we consider in this paper.

In first-generation RAN virtualization, operators have to pay for FH from the RAN to the BBU location, and then also for BH from the BBU to the EPC. The combination of FH and BH, along with the use of CPRI in the FH, greatly reduces the scope for the cost savings expected from RAN virtualization.

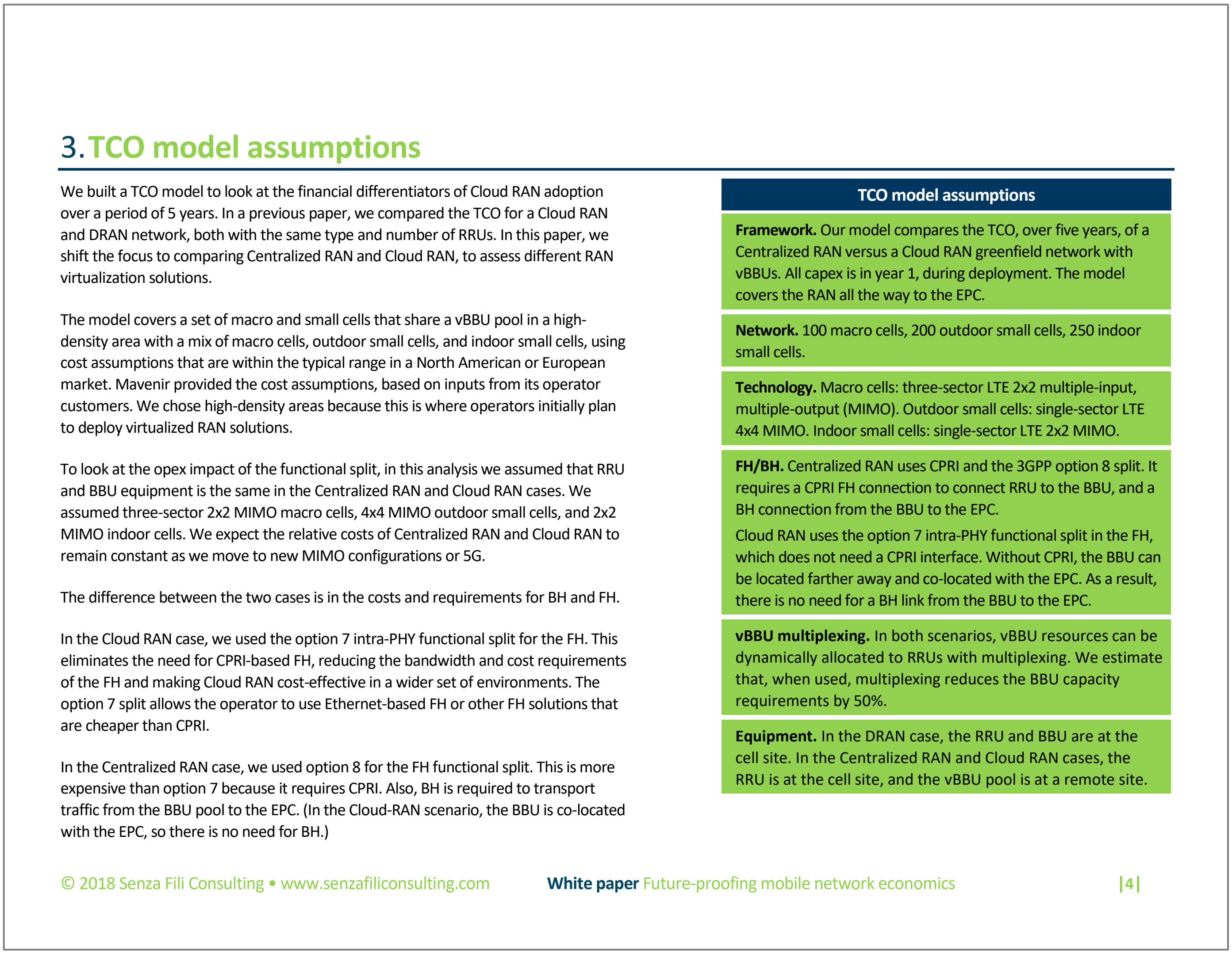
With option 8, using CPRI for FH, performance is good, but the bandwidth requirements are so high that the technology does not scale to 5G or to an increasing number of 4G cell sites. CPRI is also limited in distance: when using CPRI, operators have to locate the BBUs within 15 km of the RRU in the cell site.

Option 7, the other scenario assessed in this paper, is an intra-PHY split. It reduces the latency and bandwidth requirements. At the same time, it allows for centralized and coordinated traffic management and efficient allocation of network resources, both for today's 4G networks and for future 5G networks. According to Mavenir, option 7 requires less than 1/10 of the bandwidth than option 8 does – e.g., an FH link that requires 2.4 Gbps with option 8 would need only 170 Mbps with option 7.

We did not consider lower splits because, although they reduce the FH performance requirements and thus the overall TCO, they limit the operator's ability to use new tools to manage traffic across the virtualized RAN.

3GPP functional splits

Source: 3GPP



3. TCO model assumptions

We built a TCO model to look at the financial differentiators of Cloud RAN adoption over a period of 5 years. In a previous paper, we compared the TCO for a Cloud RAN and DRAN network, both with the same type and number of RRUs. In this paper, we shift the focus to comparing Centralized RAN and Cloud RAN, to assess different RAN virtualization solutions.

The model covers a set of macro and small cells that share a vBBU pool in a high-density area with a mix of macro cells, outdoor small cells, and indoor small cells, using cost assumptions that are within the typical range in a North American or European market. Mavenir provided the cost assumptions, based on inputs from its operator customers. We chose high-density areas because this is where operators initially plan to deploy virtualized RAN solutions.

To look at the opex impact of the functional split, in this analysis we assumed that RRU and BBU equipment is the same in the Centralized RAN and Cloud RAN cases. We assumed three-sector 2x2 MIMO macro cells, 4x4 MIMO outdoor small cells, and 2x2 MIMO indoor cells. We expect the relative costs of Centralized RAN and Cloud RAN to remain constant as we move to new MIMO configurations or 5G.

The difference between the two cases is in the costs and requirements for BH and FH.

In the Cloud RAN case, we used the option 7 intra-PHY functional split for the FH. This eliminates the need for CPRI-based FH, reducing the bandwidth and cost requirements of the FH and making Cloud RAN cost-effective in a wider set of environments. The option 7 split allows the operator to use Ethernet-based FH or other FH solutions that are cheaper than CPRI.

In the Centralized RAN case, we used option 8 for the FH functional split. This is more expensive than option 7 because it requires CPRI. Also, BH is required to transport traffic from the BBU pool to the EPC. (In the Cloud-RAN scenario, the BBU is co-located with the EPC, so there is no need for BH.)

TCO model assumptions

Framework. Our model compares the TCO, over five years, of a Centralized RAN versus a Cloud RAN greenfield network with vBBUs. All capex is in year 1, during deployment. The model covers the RAN all the way to the EPC.

Network. 100 macro cells, 200 outdoor small cells, 250 indoor small cells.

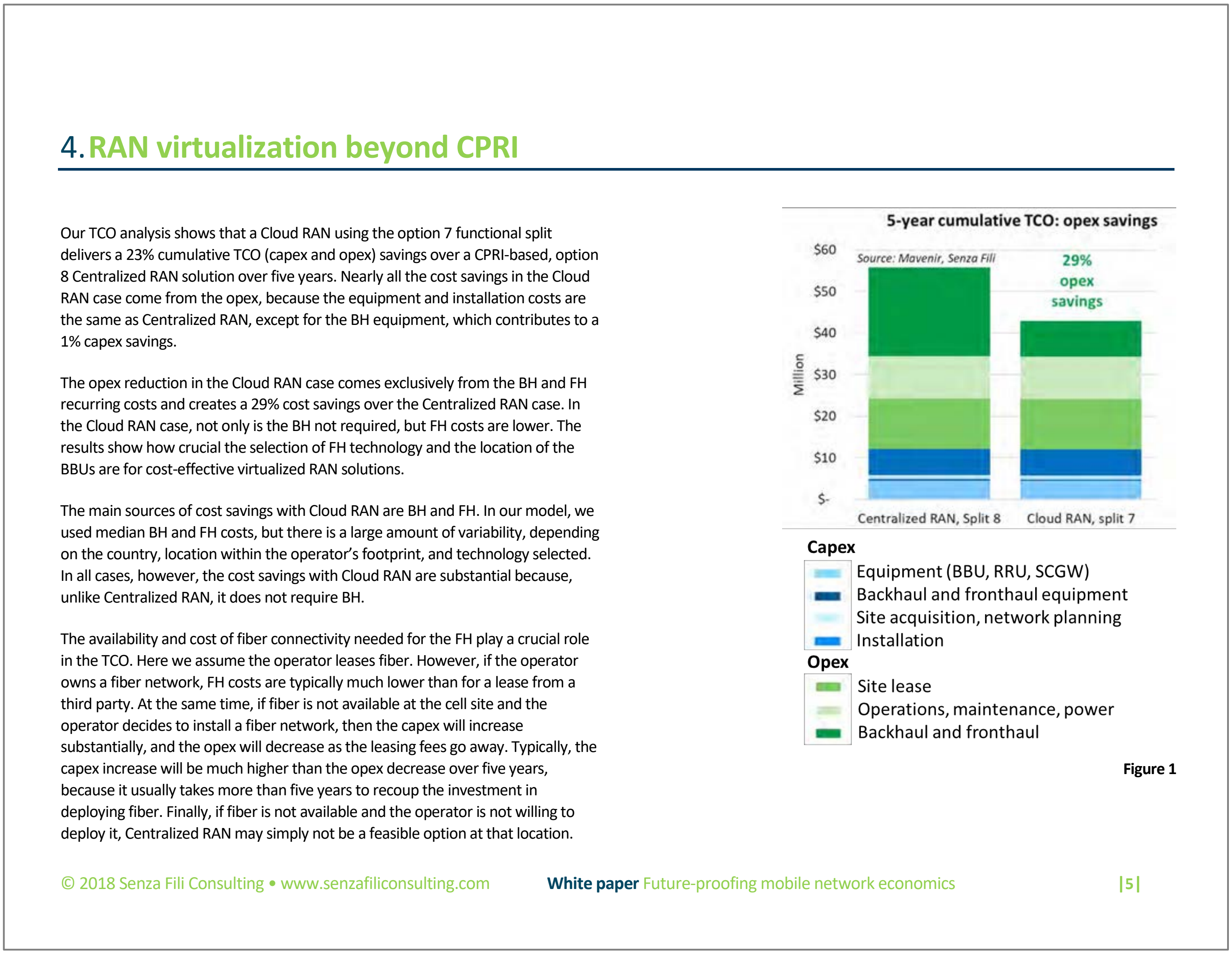
Technology. Macro cells: three-sector LTE 2x2 multiple-input, multiple-output (MIMO). Outdoor small cells: single-sector LTE 4x4 MIMO. Indoor small cells: single-sector LTE 2x2 MIMO.

FH/BH. Centralized RAN uses CPRI and the 3GPP option 8 split. It requires a CPRI FH connection to connect RRU to the BBU, and a BH connection from the BBU to the EPC.

Cloud RAN uses the option 7 intra-PHY functional split in the FH, which does not need a CPRI interface. Without CPRI, the BBU can be located farther away and co-located with the EPC. As a result, there is no need for a BH link from the BBU to the EPC.

vBBU multiplexing. In both scenarios, vBBU resources can be dynamically allocated to RRUs with multiplexing. We estimate that, when used, multiplexing reduces the BBU capacity requirements by 50%.

Equipment. In the DRAN case, the RRU and BBU are at the cell site. In the Centralized RAN and Cloud RAN cases, the RRU is at the cell site, and the vBBU pool is at a remote site.



4. RAN virtualization beyond CPRI

Our TCO analysis shows that a Cloud RAN using the option 7 functional split delivers a 23% cumulative TCO (capex and opex) savings over a CPRI-based, option 8 Centralized RAN solution over five years. Nearly all the cost savings in the Cloud RAN case come from the opex, because the equipment and installation costs are the same as Centralized RAN, except for the BH equipment, which contributes to a 1% capex savings.

The opex reduction in the Cloud RAN case comes exclusively from the BH and FH recurring costs and creates a 29% cost savings over the Centralized RAN case. In the Cloud RAN case, not only is the BH not required, but FH costs are lower. The results show how crucial the selection of FH technology and the location of the BBUs are for cost-effective virtualized RAN solutions.

The main sources of cost savings with Cloud RAN are BH and FH. In our model, we used median BH and FH costs, but there is a large amount of variability, depending on the country, location within the operator's footprint, and technology selected. In all cases, however, the cost savings with Cloud RAN are substantial because, unlike Centralized RAN, it does not require BH.

The availability and cost of fiber connectivity needed for the FH play a crucial role in the TCO. Here we assume the operator leases fiber. However, if the operator owns a fiber network, FH costs are typically much lower than for a lease from a third party. At the same time, if fiber is not available at the cell site and the operator decides to install a fiber network, then the capex will increase substantially, and the opex will decrease as the leasing fees go away. Typically, the capex increase will be much higher than the opex decrease over five years, because it usually takes more than five years to recoup the investment in deploying fiber. Finally, if fiber is not available and the operator is not willing to deploy it, Centralized RAN may simply not be a feasible option at that location.

5-year cumulative TCO: opex savings

Source: Mavenir, Senza Fili

29% opex savings

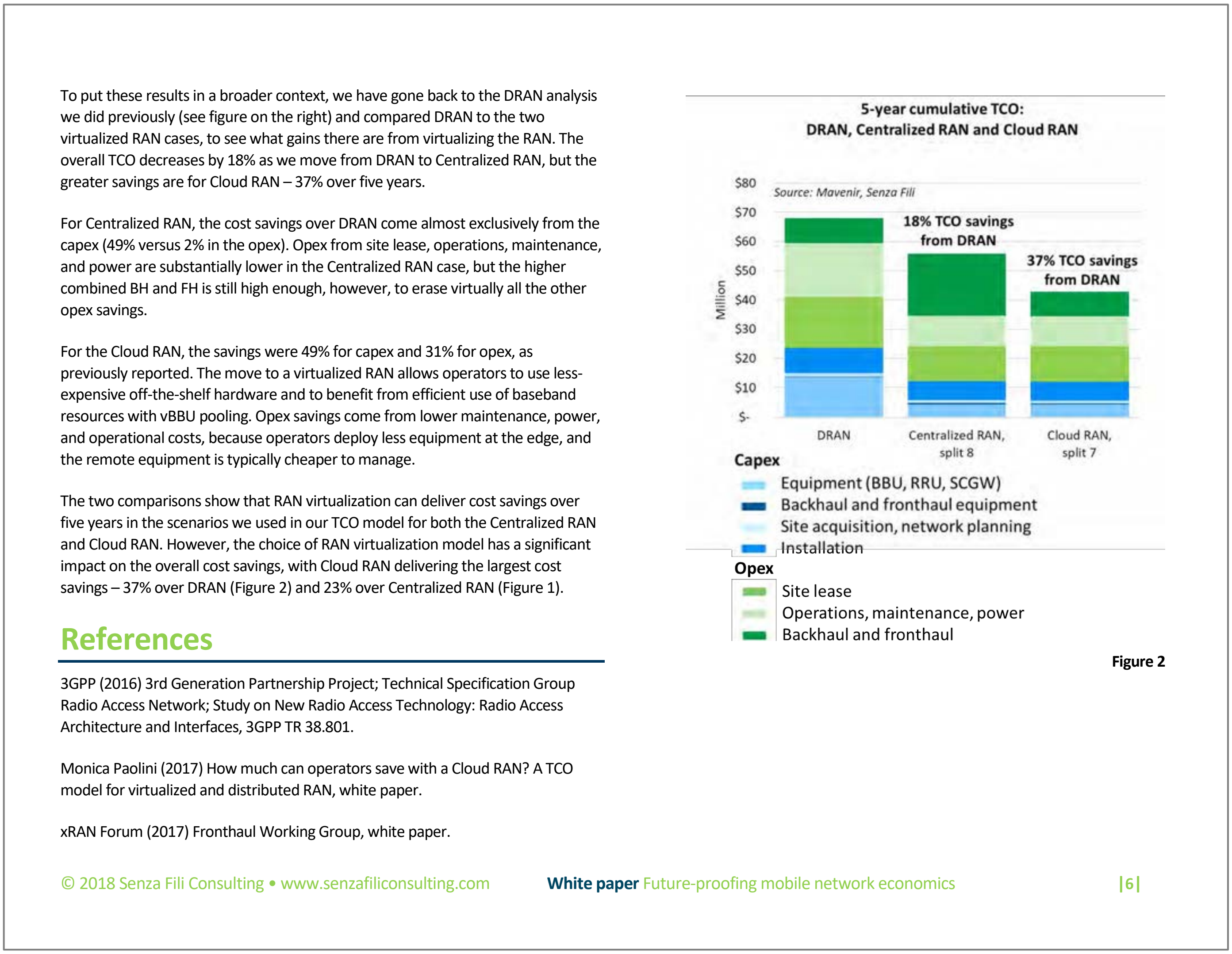
Capex

- 🟦 Equipment (BBU, RRU, SCGW)
- 🟦 Backhaul and fronthaul equipment
- 🟦 Site acquisition, network planning
- 🟦 Installation

Opex

- 🟩 Site lease
- 🟩 Operations, maintenance, power
- 🟩 Backhaul and fronthaul

Figure 1



To put these results in a broader context, we have gone back to the DRAN analysis we did previously (see figure on the right) and compared DRAN to the two virtualized RAN cases, to see what gains there are from virtualizing the RAN. The overall TCO decreases by 18% as we move from DRAN to Centralized RAN, but the greater savings are for Cloud RAN – 37% over five years.

For Centralized RAN, the cost savings over DRAN come almost exclusively from the capex (49% versus 2% in the opex). Opex from site lease, operations, maintenance, and power are substantially lower in the Centralized RAN case, but the higher combined BH and FH is still high enough, however, to erase virtually all the other opex savings.

For the Cloud RAN, the savings were 49% for capex and 31% for opex, as previously reported. The move to a virtualized RAN allows operators to use less-expensive off-the-shelf hardware and to benefit from efficient use of baseband resources with vBBU pooling. Opex savings come from lower maintenance, power, and operational costs, because operators deploy less equipment at the edge, and the remote equipment is typically cheaper to manage.

The two comparisons show that RAN virtualization can deliver cost savings over five years in the scenarios we used in our TCO model for both the Centralized RAN and Cloud RAN. However, the choice of RAN virtualization model has a significant impact on the overall cost savings, with Cloud RAN delivering the largest cost savings – 37% over DRAN (Figure 2) and 23% over Centralized RAN (Figure 1).

5-year cumulative TCO:
DRAN, Centralized RAN and Cloud RAN

Source: Mavenir, Senza Fili

$80
$70
$60
$50
$40
$30
$20
$10
$-
Million
18% TCO savings from DRAN
37% TCO savings from DRAN
DRAN
Centralized RAN, split 8
Cloud RAN, split 7
Capex
Equipment (BBU, RRU, SCGW)
Backhaul and fronthaul equipment
Site acquisition, network planning
Installation
Opex
Site lease
Operations, maintenance, power
Backhaul and fronthaul

Figure 2

References

3GPP (2016) 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Study on New Radio Access Technology: Radio Access Architecture and Interfaces, 3GPP TR 38.801.

Monica Paolini (2017) How much can operators save with a Cloud RAN? A TCO model for virtualized and distributed RAN, white paper.

xRAN Forum (2017) Fronthaul Working Group, white paper.

About Mavenir

Mavenir is purpose-built to redefine mobile network economics for Communication Service Providers (CSPs). Our innovative solutions pave the way to 5G with 100% software-based, end-to-end, Cloud Native network solutions. Leveraging industry-leading firsts in VoLTE, VoWiFi, Advanced Messaging (RCS), Multi-ID, vEPC and Cloud RAN, Mavenir accelerates network transformation for more than 250+ CSP customers in over 130 countries, serving over 50% of the world's subscribers. Mavenir embraces disruptive, innovative technology architectures and business models that drive service agility, flexibility, and velocity. With solutions that propel NFV evolution to achieve web-scale economics, Mavenir offers solutions to CSPs for cost reduction, revenue generation, and revenue protection.

About Senza Fili

Senza Fili provides advisory support on wireless data technologies and services. At Senza Fili we have in-depth expertise in financial modeling, market forecasts and research, white paper preparation, business plan support, RFP preparation and management, due diligence, and training. Our client base is international and spans the entire value chain: clients include wireline, fixed wireless, and mobile operators, enterprises and other vertical players, vendors, system integrators, investors, regulators, and industry associations. We provide a bridge between technologies and services, helping our clients assess established and emerging technologies, leverage these technologies to support new or existing services, and build solid, profitable business models. Independent advice, a strong quantitative orientation, and an international perspective are the hallmarks of our work. For additional information, visit www.senzafiliconsulting.com, or contact us at info@senzafiliconsulting.com or +1 425 657 4991.

About the Monica Paolini

Monica Paolini, Ph.D., is the founder and president of Senza Fili. She is an expert in wireless technologies and has helped clients worldwide to understand technology and customer requirements, evaluate business plan opportunities, market their services and products, and estimate the market size and revenue opportunity of new and established wireless technologies. She has frequently been invited to give presentations at conferences and has written several reports and articles on wireless broadband technologies. She has a Ph.D. in cognitive science from the University of California, San Diego (US), an MBA from the University of Oxford (UK), and a BA/MA in philosophy from the University of Bologna (Italy). You can contact Monica at monica.paolini@senzafiliconsulting.com.

© 2018 Senza Fili Consulting LLC. All rights reserved. This white paper was prepared on behalf of Mavenir. The views and statements expressed in the white paper are those of Senza Fili, and they should not be inferred to reflect the position of Mavenir. The document can be distributed only in its integral form and acknowledging the source. No selection of this material may be copied, photocopied, or duplicated in any form or by any means, or redistributed without express written permission from Senza Fili. While the document relies on information that we consider accurate and reliable, Senza Fili makes no warranty, express or implied, as to the accuracy of the information in this document. Senza Fili assumes no liability for any damage or loss arising from reliance on this information. Trademarks mentioned in this document are the property of their respective owners. Cover page photo by chuyuss/Shutterstock.

How much can operators save with a Cloud RAN?

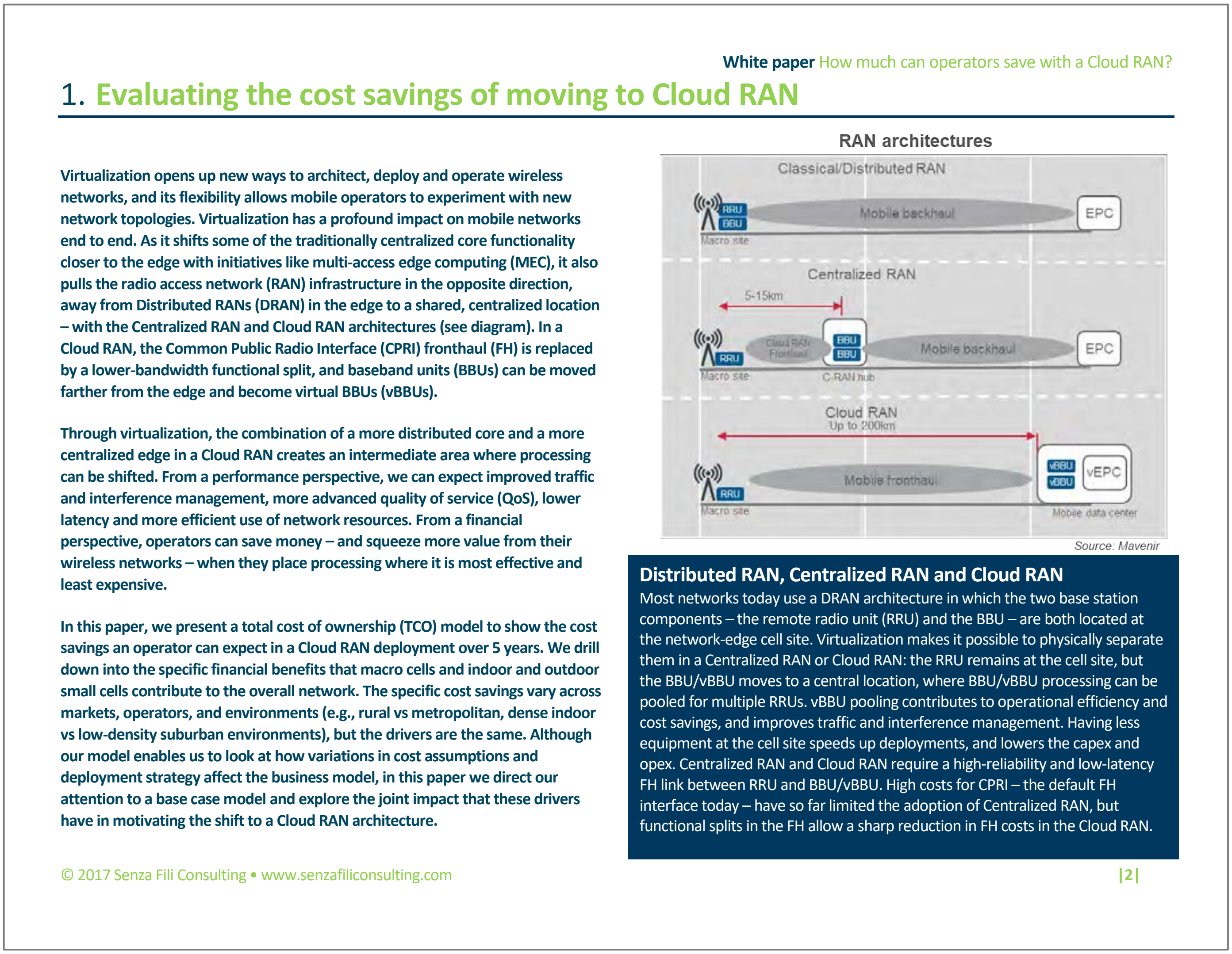
A TCO model for virtualized and distributed RAN

By Monica Paolini
Senza Fili

SENZA FILI

Sponsored by

MAVENIR



1. Evaluating the cost savings of moving to Cloud RAN

Virtualization opens up new ways to architect, deploy and operate wireless networks, and its flexibility allows mobile operators to experiment with new network topologies. Virtualization has a profound impact on mobile networks end to end. As it shifts some of the traditionally centralized core functionality closer to the edge with initiatives like multi-access edge computing (MEC), it also pulls the radio access network (RAN) infrastructure in the opposite direction, away from Distributed RANs (DRAN) in the edge to a shared, centralized location – with the Centralized RAN and Cloud RAN architectures (see diagram). In a Cloud RAN, the Common Public Radio Interface (CPRI) fronthaul (FH) is replaced by a lower-bandwidth functional split, and baseband units (BBUs) can be moved farther from the edge and become virtual BBUs (vBBUs).

Through virtualization, the combination of a more distributed core and a more centralized edge in a Cloud RAN creates an intermediate area where processing can be shifted. From a performance perspective, we can expect improved traffic and interference management, more advanced quality of service (QoS), lower latency and more efficient use of network resources. From a financial perspective, operators can save money – and squeeze more value from their wireless networks – when they place processing where it is most effective and least expensive.

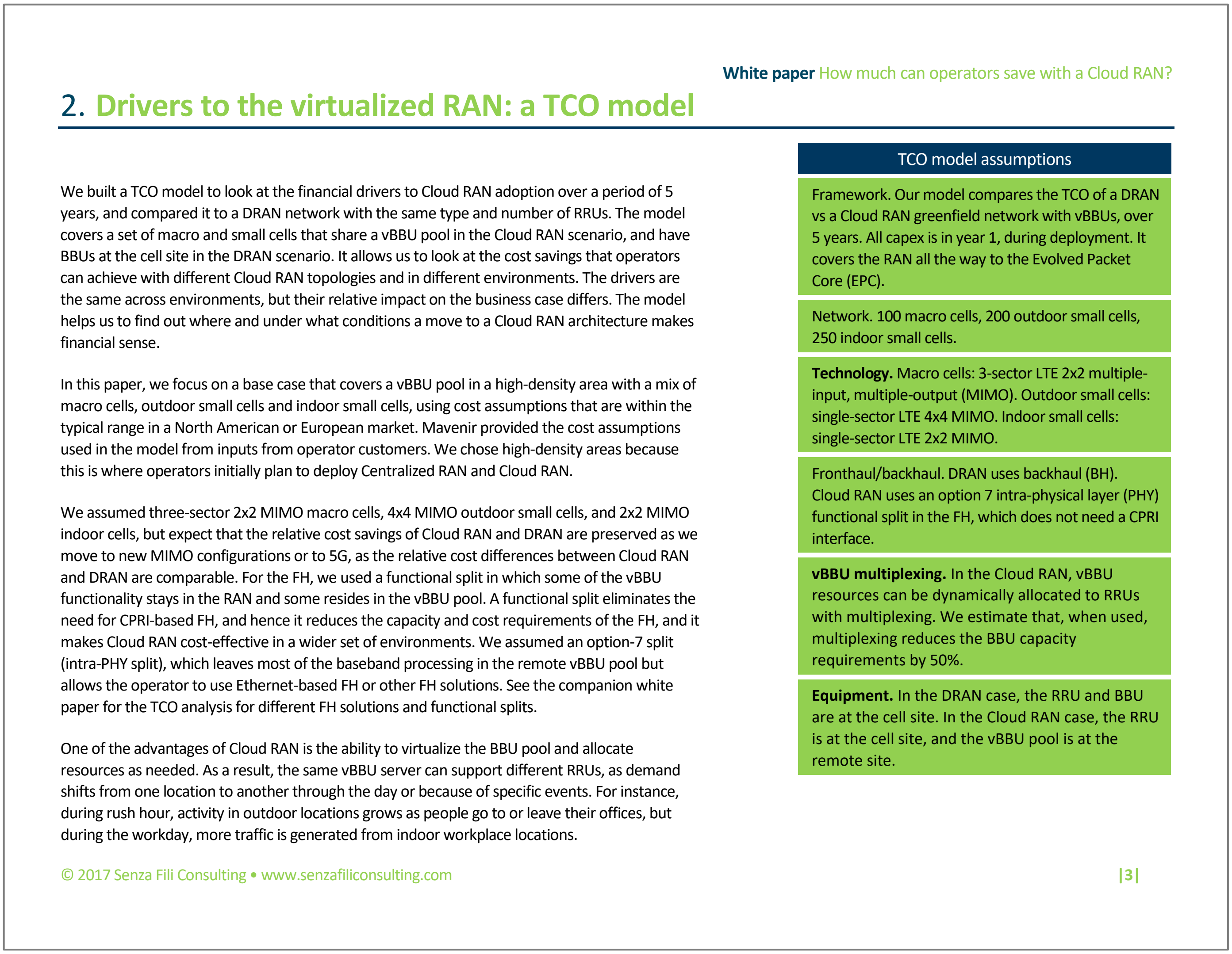
In this paper, we present a total cost of ownership (TCO) model to show the cost savings an operator can expect in a Cloud RAN deployment over 5 years. We drill down into the specific financial benefits that macro cells and indoor and outdoor small cells contribute to the overall network. The specific cost savings vary across markets, operators, and environments (e.g., rural vs metropolitan, dense indoor vs low-density suburban environments), but the drivers are the same. Although our model enables us to look at how variations in cost assumptions and deployment strategy affect the business model, in this paper we direct our attention to a base case model and explore the joint impact that these drivers have in motivating the shift to a Cloud RAN architecture.

RAN architectures

Source: Mavenir

Distributed RAN, Centralized RAN and Cloud RAN

Most networks today use a DRAN architecture in which the two base station components – the remote radio unit (RRU) and the BBU – are both located at the network-edge cell site. Virtualization makes it possible to physically separate them in a Centralized RAN or Cloud RAN: the RRU remains at the cell site, but the BBU/vBBU moves to a central location, where BBU/vBBU processing can be pooled for multiple RRUs. vBBU pooling contributes to operational efficiency and cost savings, and improves traffic and interference management. Having less equipment at the cell site speeds up deployments, and lowers the capex and opex. Centralized RAN and Cloud RAN require a high-reliability and low-latency FH link between RRU and BBU/vBBU. High costs for CPRI – the default FH interface today – have so far limited the adoption of Centralized RAN, but functional splits in the FH allow a sharp reduction in FH costs in the Cloud RAN.



2. Drivers to the virtualized RAN: a TCO model

We built a TCO model to look at the financial drivers to Cloud RAN adoption over a period of 5 years, and compared it to a DRAN network with the same type and number of RRUs. The model covers a set of macro and small cells that share a vBBU pool in the Cloud RAN scenario, and have BBUs at the cell site in the DRAN scenario. It allows us to look at the cost savings that operators can achieve with different Cloud RAN topologies and in different environments. The drivers are the same across environments, but their relative impact on the business case differs. The model helps us to find out where and under what conditions a move to a Cloud RAN architecture makes financial sense.

In this paper, we focus on a base case that covers a vBBU pool in a high-density area with a mix of macro cells, outdoor small cells and indoor small cells, using cost assumptions that are within the typical range in a North American or European market. Mavenir provided the cost assumptions used in the model from inputs from operator customers. We chose high-density areas because this is where operators initially plan to deploy Centralized RAN and Cloud RAN.

We assumed three-sector 2x2 MIMO macro cells, 4x4 MIMO outdoor small cells, and 2x2 MIMO indoor cells, but expect that the relative cost savings of Cloud RAN and DRAN are preserved as we move to new MIMO configurations or to 5G, as the relative cost differences between Cloud RAN and DRAN are comparable. For the FH, we used a functional split in which some of the vBBU functionality stays in the RAN and some resides in the vBBU pool. A functional split eliminates the need for CPRI-based FH, and hence it reduces the capacity and cost requirements of the FH, and it makes Cloud RAN cost-effective in a wider set of environments. We assumed an option-7 split (intra-PHY split), which leaves most of the baseband processing in the remote vBBU pool but allows the operator to use Ethernet-based FH or other FH solutions. See the companion white paper for the TCO analysis for different FH solutions and functional splits.

One of the advantages of Cloud RAN is the ability to virtualize the BBU pool and allocate resources as needed. As a result, the same vBBU server can support different RRUs, as demand shifts from one location to another through the day or because of specific events. For instance, during rush hour, activity in outdoor locations grows as people go to or leave their offices, but during the workday, more traffic is generated from indoor workplace locations.

TCO model assumptions

Framework. Our model compares the TCO of a DRAN vs a Cloud RAN greenfield network with vBBUs, over 5 years. All capex is in year 1, during deployment. It covers the RAN all the way to the Evolved Packet Core (EPC).

Network. 100 macro cells, 200 outdoor small cells, 250 indoor small cells.

Technology. Macro cells: 3-sector LTE 2x2 multiple-input, multiple-output (MIMO). Outdoor small cells: single-sector LTE 4x4 MIMO. Indoor small cells: single-sector LTE 2x2 MIMO.

Fronthaul/backhaul. DRAN uses backhaul (BH). Cloud RAN uses an option 7 intra-physical layer (PHY) functional split in the FH, which does not need a CPRI interface.

vBBU multiplexing. In the Cloud RAN, vBBU resources can be dynamically allocated to RRUs with multiplexing. We estimate that, when used, multiplexing reduces the BBU capacity requirements by 50%.

Equipment. In the DRAN case, the RRU and BBU are at the cell site. In the Cloud RAN case, the RRU is at the cell site, and the vBBU pool is at the remote site.

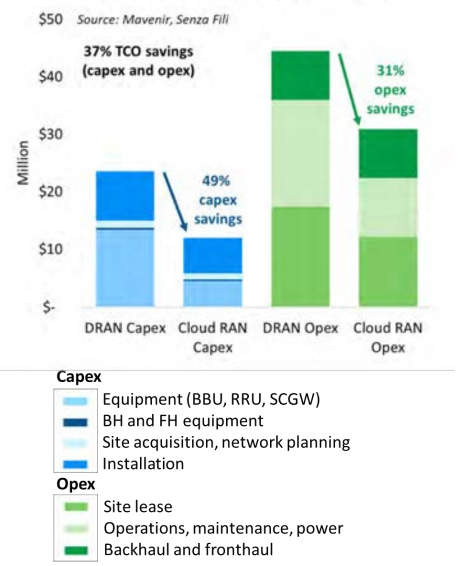
3. Cloud RAN can save 37% in costs compared with DRAN

The base case in our TCO model demonstrates a 37% reduction in deployment and operational costs over 5 years, from a 49% savings in capex in year 1 and a cumulative 31% savings in opex over the 5 years.

Capex savings primarily come from a reduction in equipment costs in the vBBU. The RRU costs are largely the same in both the DRAN and Cloud RAN scenarios, but the vBBU costs are lower in the Cloud RAN scenario because the BBUs are virtualized. Virtualization makes it possible to use both less-expensive non-proprietary hardware, and BBU pooling. With pooling, the efficiency in the use of vBBU resources increases, and the vBBU pool needs less baseband processing capacity (and hence less hardware). The reduced need for equipment at the cell site not only lowers capex, it enables faster deployment and more flexibility of equipment location. Planning and installation are also cheaper for Cloud RAN, but the cost reduction for them is less pronounced, because mobile operators still have to deploy the RRU at the edge.

Opex savings are mostly due to the reduction in maintenance, power and operations costs, in more-centralized vBBU locations that are typically easier to access and cheaper to operate. Leases at the cell site also cost less, because of the reduction in equipment located there. Because the model assumes a functional split, we assumed the cost for the FH in the Cloud RAN scenario to be the same as the cost for BH in the DRAN scenario. Had a CPRI-based FH been used instead, the Cloud RAN FH costs would have been substantially higher, and the opex savings reduced – to 11%, from the 31% we demonstrated in the base case.

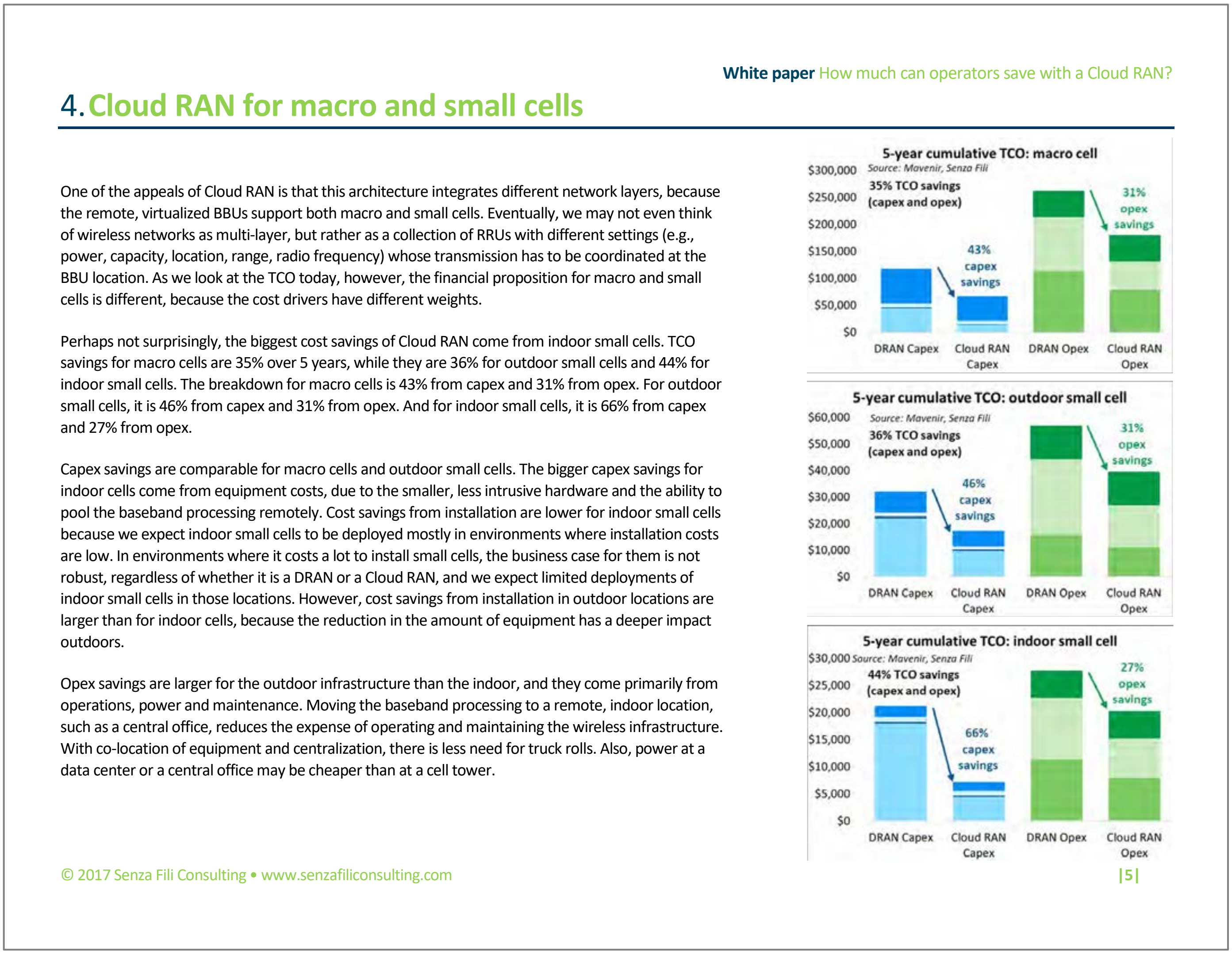
5-year cumulative TCO: capex and opex



Source: Mavenir, Senza Fili

Beyond the TCO base case

Our TCO model focuses on a base case that reflects cost savings levels that mobile operators can achieve in many markets. However, in addition to the cost savings, operators stand to benefit from improved performance. Improved performance does not lower the TCO, but lowers per-bit costs (and can improve revenues and QoE). To keep the assessment conservative, we have excluded the performance gains from the TCO base case. Also, operators that own, or otherwise have low-cost access to, an FH/BH network can significantly lower their operational costs. In a scenario in which the operator has free access to FH/BH, the cost savings can reach 42% (an increase from 31% in the base case). A neutral-host model can also lower costs to an individual operator, because operators can share the costs of the network deployment and operations with other operators. In a Cloud RAN neutral-host scenario, we project 48% TCO savings (54% from capex, 45% from opex).



4. Cloud RAN for macro and small cells

One of the appeals of Cloud RAN is that this architecture integrates different network layers, because the remote, virtualized BBUs support both macro and small cells. Eventually, we may not even think of wireless networks as multi-layer, but rather as a collection of RRUs with different settings (e.g., power, capacity, location, range, radio frequency) whose transmission has to be coordinated at the BBU location. As we look at the TCO today, however, the financial proposition for macro and small cells is different, because the cost drivers have different weights.

Perhaps not surprisingly, the biggest cost savings of Cloud RAN come from indoor small cells. TCO savings for macro cells are 35% over 5 years, while they are 36% for outdoor small cells and 44% for indoor small cells. The breakdown for macro cells is 43% from capex and 31% from opex. For outdoor small cells, it is 46% from capex and 31% from opex. And for indoor small cells, it is 66% from capex and 27% from opex.

Capex savings are comparable for macro cells and outdoor small cells. The bigger capex savings for indoor cells come from equipment costs, due to the smaller, less intrusive hardware and the ability to pool the baseband processing remotely. Cost savings from installation are lower for indoor small cells because we expect indoor small cells to be deployed mostly in environments where installation costs are low. In environments where it costs a lot to install small cells, the business case for them is not robust, regardless of whether it is a DRAN or a Cloud RAN, and we expect limited deployments of indoor small cells in those locations. However, cost savings from installation in outdoor locations are larger than for indoor cells, because the reduction in the amount of equipment has a deeper impact outdoors.

Opex savings are larger for the outdoor infrastructure than the indoor, and they come primarily from operations, power and maintenance. Moving the baseband processing to a remote, indoor location, such as a central office, reduces the expense of operating and maintaining the wireless infrastructure. With co-location of equipment and centralization, there is less need for truck rolls. Also, power at a data center or a central office may be cheaper than at a cell tower.

5-year cumulative TCO: macro cell

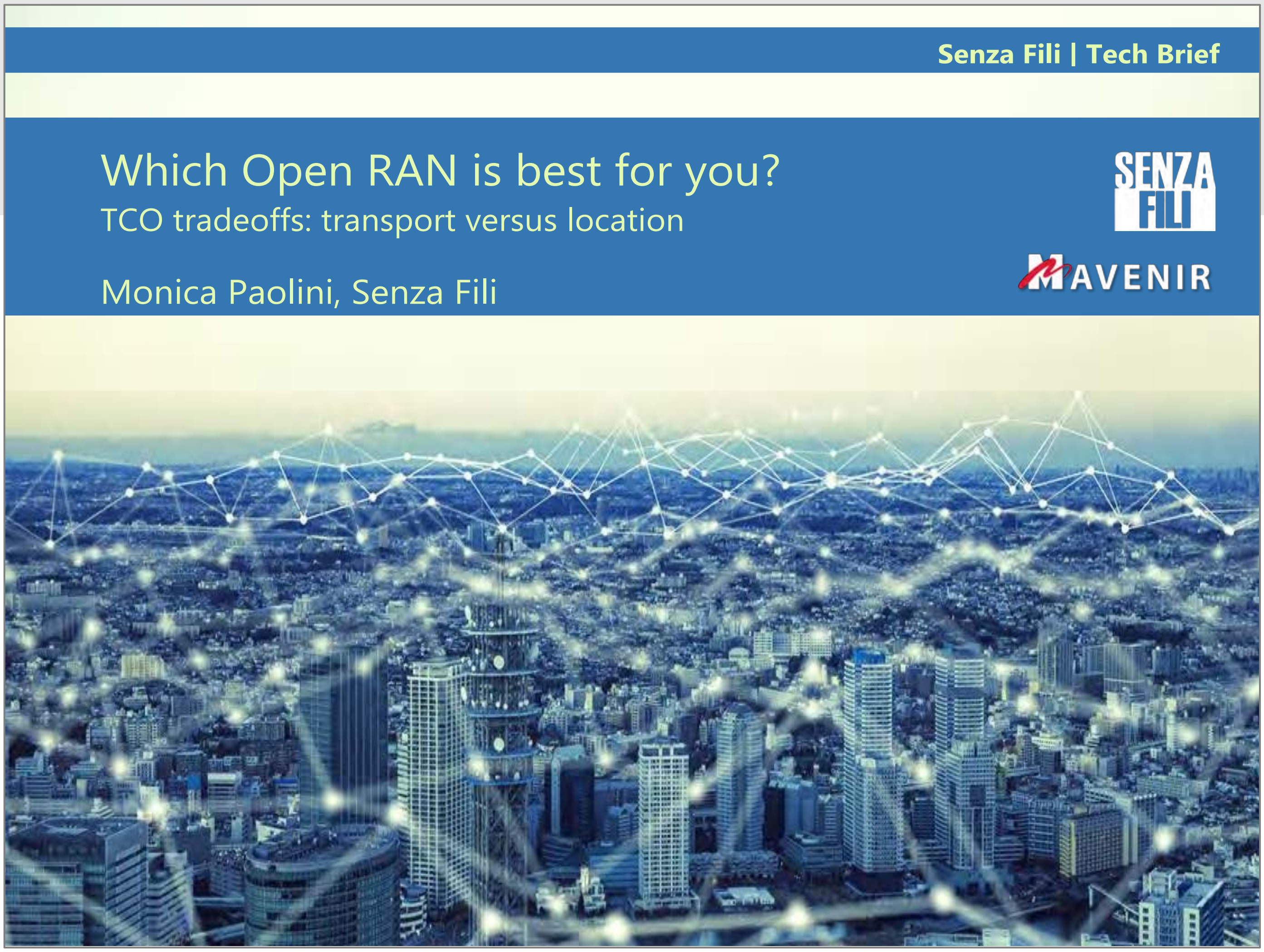
Source: Mavenir, Senza Fili

5-year cumulative TCO: outdoor small cell

Source: Mavenir, Senza Fili

5-year cumulative TCO: indoor small cell

Source: Mavenir, Senza Fili

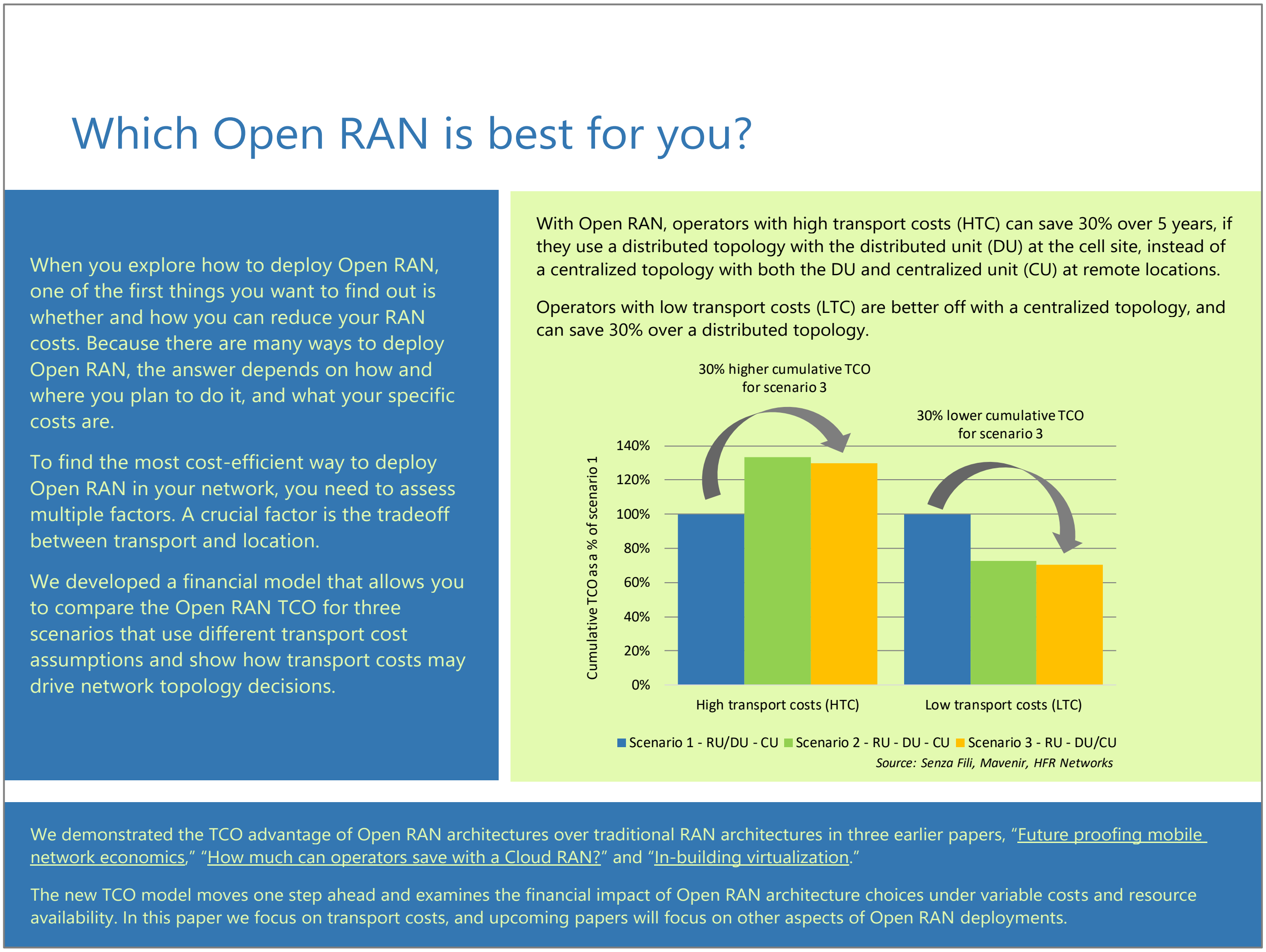


Senza Fili | Tech Brief

Which Open RAN is best for you?

TCO tradeoffs: transport versus location

Monica Paolini, Senza Fili



Which Open RAN is best for you?

When you explore how to deploy Open RAN, one of the first things you want to find out is whether and how you can reduce your RAN costs. Because there are many ways to deploy Open RAN, the answer depends on how and where you plan to do it, and what your specific costs are.

To find the most cost-efficient way to deploy Open RAN in your network, you need to assess multiple factors. A crucial factor is the tradeoff between transport and location.

We developed a financial model that allows you to compare the Open RAN TCO for three scenarios that use different transport cost assumptions and show how transport costs may drive network topology decisions.

With Open RAN, operators with high transport costs (HTC) can save 30% over 5 years, if they use a distributed topology with the distributed unit (DU) at the cell site, instead of a centralized topology with both the DU and centralized unit (CU) at remote locations.

Operators with low transport costs (LTC) are better off with a centralized topology, and can save 30% over a distributed topology.

30% higher cumulative TCO for scenario 3
30% lower cumulative TCO for scenario 3
Cumulative TCO as a % of scenario 1
140%
120%
100%
80%
60%
40%
20%
0%
High transport costs (HTC)
Low transport costs (LTC)
■ Scenario 1 - RU/DU - CU
■ Scenario 2 - RU - DU - CU
■ Scenario 3 - RU - DU/CU

Source: Senza Fili, Mavenir, HFR Networks

We demonstrated the TCO advantage of Open RAN architectures over traditional RAN architectures in three earlier papers, "Future proofing mobile network economics," "How much can operators save with a Cloud RAN?" and "In-building virtualization."

The new TCO model moves one step ahead and examines the financial impact of Open RAN architecture choices under variable costs and resource availability. In this paper we focus on transport costs, and upcoming papers will focus on other aspects of Open RAN deployments.

Open RAN gives operators flexibility in how they architect their RAN, allowing them to have distributed topologies with more hardware and processing toward the edge, and centralized topologies with DUs and CUs in remote locations in data centers.

The location-related costs vary across locations and operators. They depend on capex items such as site acquisition, deployment and data center set-up fees, and to a larger extent on opex items such as site leases, maintenance and power.

At the same time, transport costs may vary even more than location-related costs. As a result, the higher transport costs due to demanding fronthaul (FH) requirements increase the TCO in a centralized architecture.

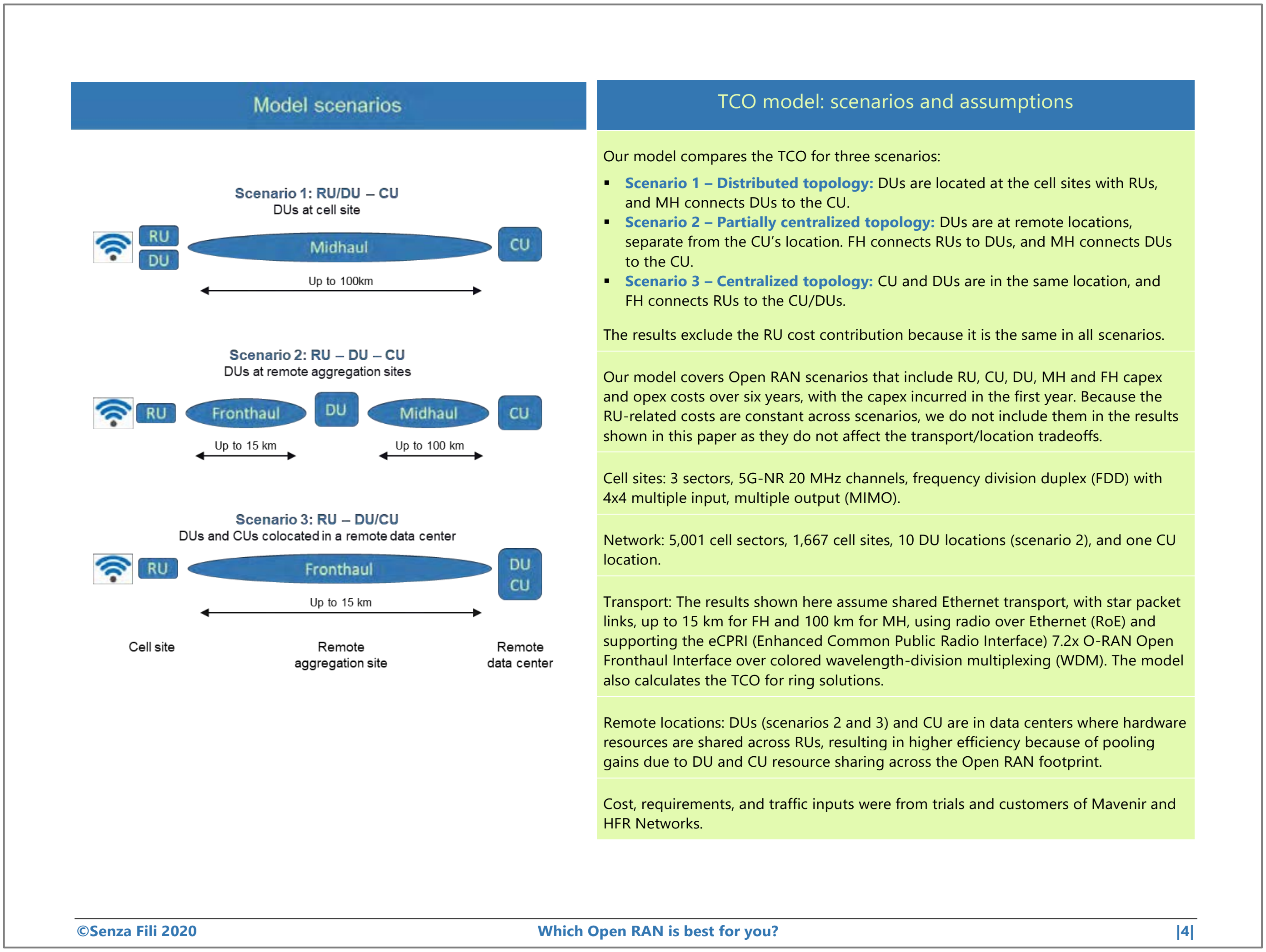
We compared the location/transport tradeoffs in distributed and centralized architectures by keeping the location costs constant and varying the transport costs.

Our base case – high transport costs (HTC) – is more likely to apply to a brownfield mobile operator that does not own the transport infrastructure and has to pay market prices for transport. The low-transport-cost (LTC) case is more typical of an operator that owns a transport network and hence has a low transport cost basis.

Because the only difference between the HTC and LTC cases is transport costs (i.e., $1,000 and $100 per month for a one Gbps link, respectively, with per-Gbps costs declining as link capacity goes up), the overall TCO for the HTC case is higher than for the LTC case.

The next pages show the TCO results for both the HTC and LTC cases. The difference in transport costs determines which of three scenarios is more cost efficient. If transport costs are high, having the DU at the cell site (scenario 1) is the lowest-cost option. If transport costs are low, locating both the DU and CU in remote locations (scenario 2 and 3) reduces costs.

In some cases, locating the DU and CU at the same locations may not be a desirable topology. For instance, the DU location may be too far away from the cell site and there are limitations to the length of a fronthaul link. If DU and CU are not in the same remote location (scenario 2), there is a slight cost increase over scenario 3, due to the need to support more locations and for midhaul (MH) connections from the DU to the CU site. The choice between scenarios 2 and 3 will most likely be dependent on topology constraints (e.g., cell site locations and density, or distance to the CU), rather than cost considerations.



Model scenarios

TCO model: scenarios and assumptions

Our model compares the TCO for three scenarios:

- **Scenario 1 – Distributed topology:** DUs are located at the cell sites with RUs, and MH connects DUs to the CU.
- **Scenario 2 – Partially centralized topology:** DUs are at remote locations, separate from the CU's location. FH connects RUs to DUs, and MH connects DUs to the CU.
- **Scenario 3 – Centralized topology:** CU and DUs are in the same location, and FH connects RUs to the CU/DUs.

The results exclude the RU cost contribution because it is the same in all scenarios.

Our model covers Open RAN scenarios that include RU, CU, DU, MH and FH capex and opex costs over six years, with the capex incurred in the first year. Because the RU-related costs are constant across scenarios, we do not include them in the results shown in this paper as they do not affect the transport/location tradeoffs.

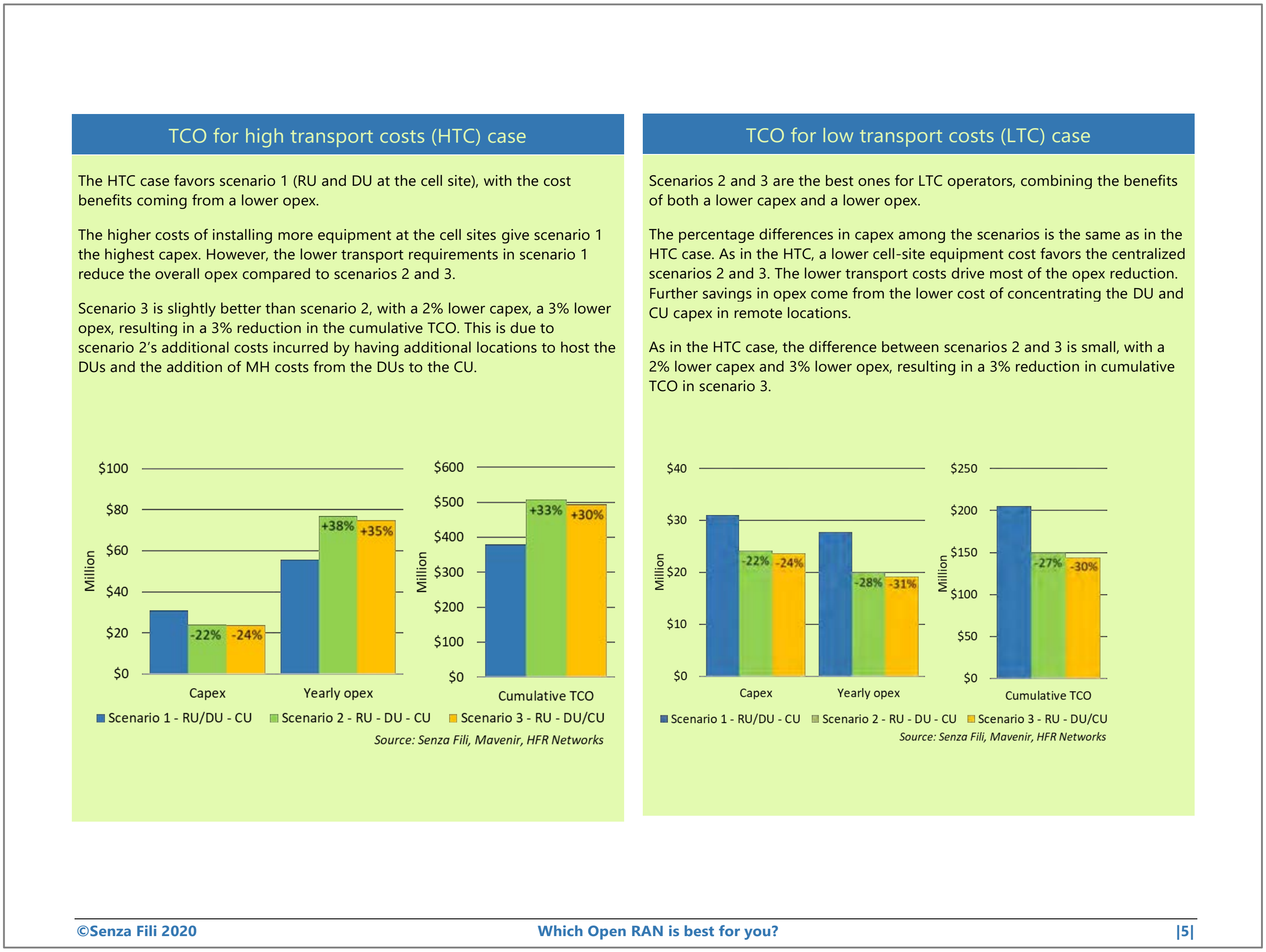
Cell sites: 3 sectors, 5G-NR 20 MHz channels, frequency division duplex (FDD) with 4x4 multiple input, multiple output (MIMO).

Network: 5,001 cell sectors, 1,667 cell sites, 10 DU locations (scenario 2), and one CU location.

Transport: The results shown here assume shared Ethernet transport, with star packet links, up to 15 km for FH and 100 km for MH, using radio over Ethernet (RoE) and supporting the eCPRI (Enhanced Common Public Radio Interface) 7.2x O-RAN Open Fronthaul Interface over colored wavelength-division multiplexing (WDM). The model also calculates the TCO for ring solutions.

Remote locations: DUs (scenarios 2 and 3) and CU are in data centers where hardware resources are shared across RUs, resulting in higher efficiency because of pooling gains due to DU and CU resource sharing across the Open RAN footprint.

Cost, requirements, and traffic inputs were from trials and customers of Mavenir and HFR Networks.



TCO for high transport costs (HTC) case

The HTC case favors scenario 1 (RU and DU at the cell site), with the cost benefits coming from a lower opex.

The higher costs of installing more equipment at the cell sites give scenario 1 the highest capex. However, the lower transport requirements in scenario 1 reduce the overall opex compared to scenarios 2 and 3.

Scenario 3 is slightly better than scenario 2, with a 2% lower capex, a 3% lower opex, resulting in a 3% reduction in the cumulative TCO. This is due to scenario 2's additional costs incurred by having additional locations to host the DUs and the addition of MH costs from the DUs to the CU.

Source: Senza Fili, Mavenir, HFR Networks

TCO for low transport costs (LTC) case

Scenarios 2 and 3 are the best ones for LTC operators, combining the benefits of both a lower capex and a lower opex.

The percentage differences in capex among the scenarios is the same as in the HTC case. As in the HTC, a lower cell-site equipment cost favors the centralized scenarios 2 and 3. The lower transport costs drive most of the opex reduction. Further savings in opex come from the lower cost of concentrating the DU and CU capex in remote locations.

As in the HTC case, the difference between scenarios 2 and 3 is small, with a 2% lower capex and 3% lower opex, resulting in a 3% reduction in cumulative TCO in scenario 3.

Source: Senza Fili, Mavenir, HFR Networks

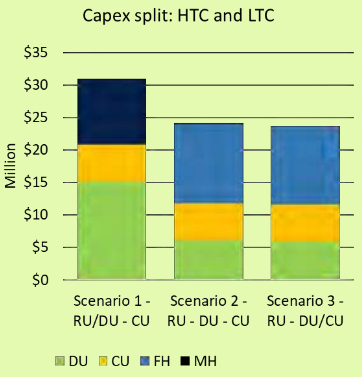
Comparing opex and capex in the HTC and LTC cases

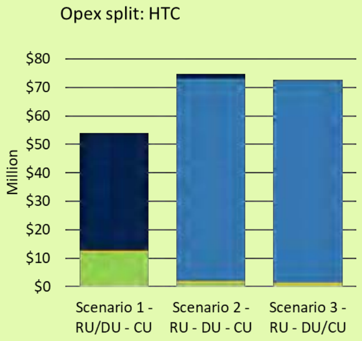
The capex in both the HTC and LTC cases is the same. Across scenarios, the major difference is in the DU costs are 60% and 61% lower in scenarios 2 and 3, respectively, than in scenario 1, which has higher installation costs and hardware costs. CU costs are the same, because the CU is located remotely in one location in all scenarios. For the combined FH and MH transport, scenario 1 has the lowest capex because it requires only MH; scenario 2 is 22% higher because of its MH/FH combination, and scenario 3, using FH only, is 19% higher than scenario 1.

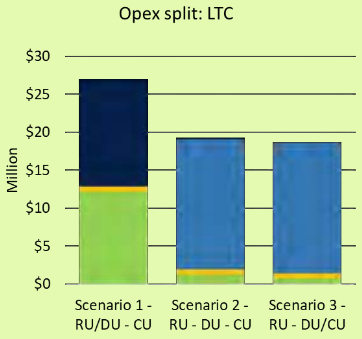
Not only does the opex total change across scenarios and across the HTC and LTC cases, its composition changes as well.

In the HTC case, transport costs account for a larger share of the opex: 76%, 97% and 98% in the three scenarios, respectively. The higher share of transport costs in scenarios 2 and 3 is due to the higher transport requirements from FH.

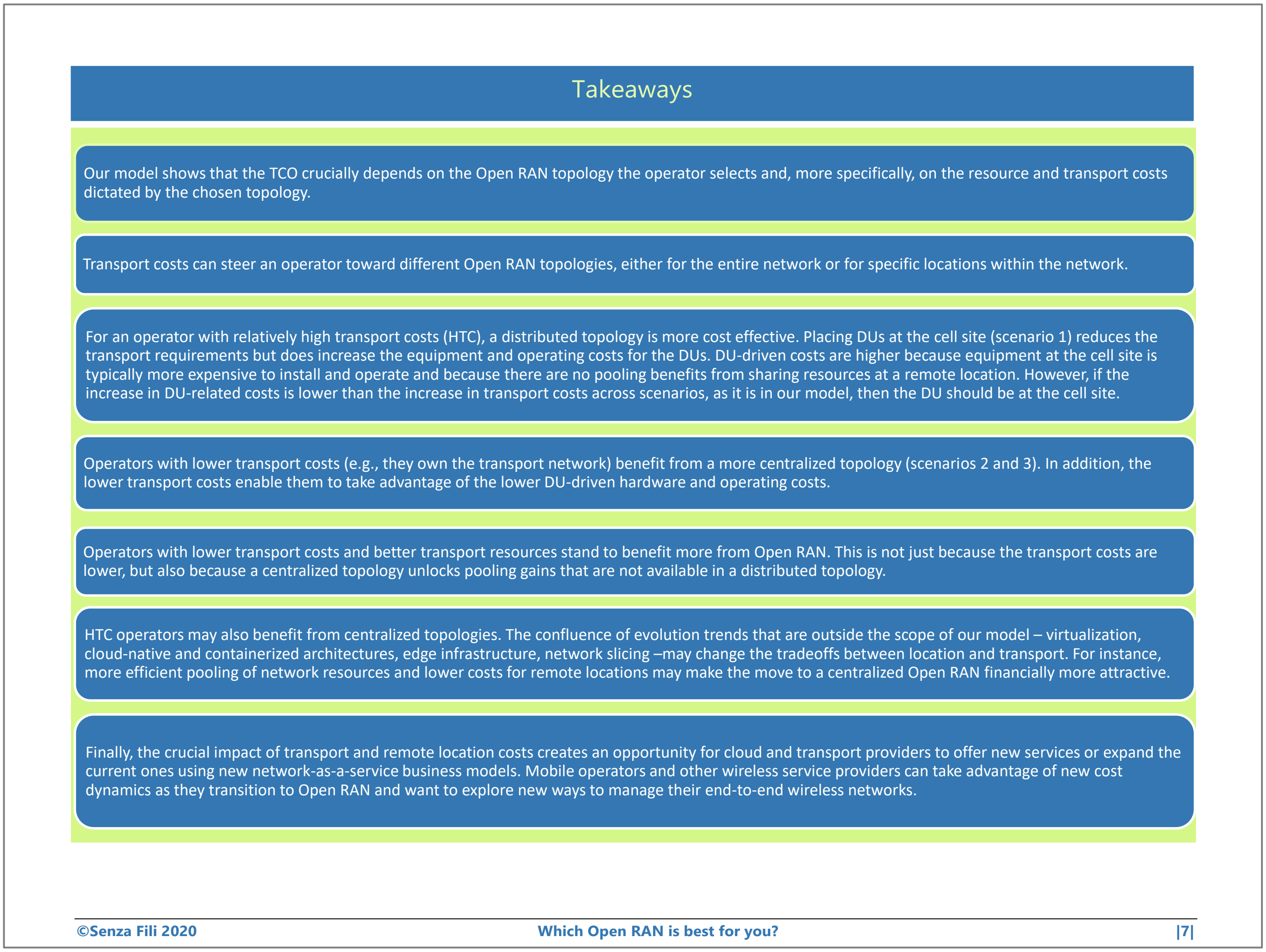
In the LTC case, DU costs also play a larger role across all scenarios, with DU costs accounting for 45% of opex in scenario 1, 7% in scenario 2, and 4% in scenario 3. Transport costs account for 52% of opex in scenario 1, 90% in scenario 2, and 92% in scenario 3.







Source: Senza Fili, Mavenir, HFR Networks



Takeaways

Our model shows that the TCO crucially depends on the Open RAN topology the operator selects and, more specifically, on the resource and transport costs dictated by the chosen topology.

Transport costs can steer an operator toward different Open RAN topologies, either for the entire network or for specific locations within the network.

For an operator with relatively high transport costs (HTC), a distributed topology is more cost effective. Placing DUs at the cell site (scenario 1) reduces the transport requirements but does increase the equipment and operating costs for the DUs. DU-driven costs are higher because equipment at the cell site is typically more expensive to install and operate and because there are no pooling benefits from sharing resources at a remote location. However, if the increase in DU-related costs is lower than the increase in transport costs across scenarios, as it is in our model, then the DU should be at the cell site.

Operators with lower transport costs (e.g., they own the transport network) benefit from a more centralized topology (scenarios 2 and 3). In addition, the lower transport costs enable them to take advantage of the lower DU-driven hardware and operating costs.

Operators with lower transport costs and better transport resources stand to benefit more from Open RAN. This is not just because the transport costs are lower, but also because a centralized topology unlocks pooling gains that are not available in a distributed topology.

HTC operators may also benefit from centralized topologies. The confluence of evolution trends that are outside the scope of our model – virtualization, cloud-native and containerized architectures, edge infrastructure, network slicing –may change the tradeoffs between location and transport. For instance, more efficient pooling of network resources and lower costs for remote locations may make the move to a centralized Open RAN financially more attractive.

Finally, the crucial impact of transport and remote location costs creates an opportunity for cloud and transport providers to offer new services or expand the current ones using new network-as-a-service business models. Mobile operators and other wireless service providers can take advantage of new cost dynamics as they transition to Open RAN and want to explore new ways to manage their end-to-end wireless networks.

In-building virtualization

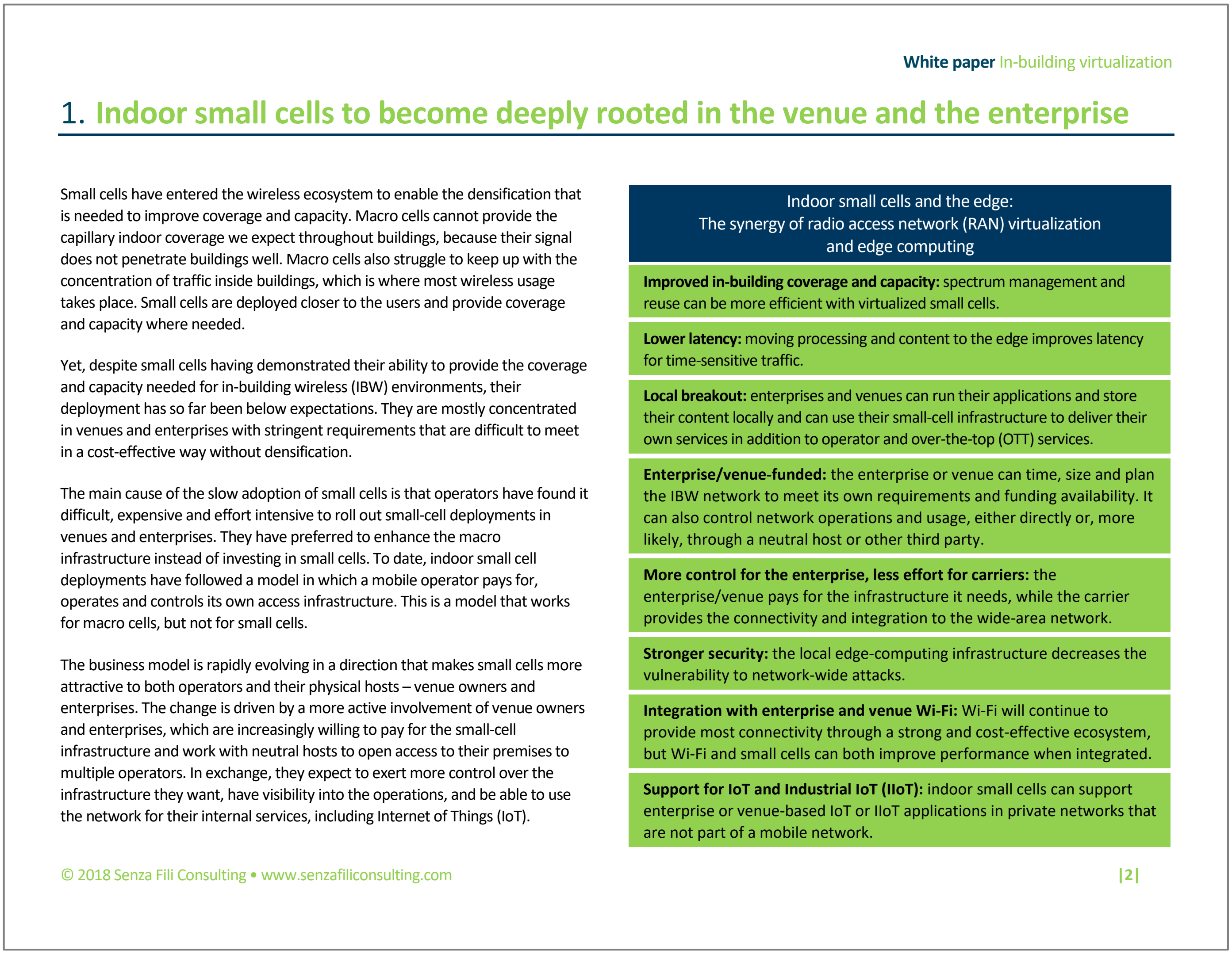
An assessment of the TCO for virtualized indoor small cells

By Monica Paolini
Senza Fili

SENZA FILI

Sponsored by

MAVENIR



1. Indoor small cells to become deeply rooted in the venue and the enterprise

Small cells have entered the wireless ecosystem to enable the densification that is needed to improve coverage and capacity. Macro cells cannot provide the capillary indoor coverage we expect throughout buildings, because their signal does not penetrate buildings well. Macro cells also struggle to keep up with the concentration of traffic inside buildings, which is where most wireless usage takes place. Small cells are deployed closer to the users and provide coverage and capacity where needed.

Yet, despite small cells having demonstrated their ability to provide the coverage and capacity needed for in-building wireless (IBW) environments, their deployment has so far been below expectations. They are mostly concentrated in venues and enterprises with stringent requirements that are difficult to meet in a cost-effective way without densification.

The main cause of the slow adoption of small cells is that operators have found it difficult, expensive and effort intensive to roll out small-cell deployments in venues and enterprises. They have preferred to enhance the macro infrastructure instead of investing in small cells. To date, indoor small cell deployments have followed a model in which a mobile operator pays for, operates and controls its own access infrastructure. This is a model that works for macro cells, but not for small cells.

The business model is rapidly evolving in a direction that makes small cells more attractive to both operators and their physical hosts – venue owners and enterprises. The change is driven by a more active involvement of venue owners and enterprises, which are increasingly willing to pay for the small-cell infrastructure and work with neutral hosts to open access to their premises to multiple operators. In exchange, they expect to exert more control over the infrastructure they want, have visibility into the operations, and be able to use the network for their internal services, including Internet of Things (IoT).

Indoor small cells and the edge:
The synergy of radio access network (RAN) virtualization
and edge computing

Improved in-building coverage and capacity: spectrum management and reuse can be more efficient with virtualized small cells.

Lower latency: moving processing and content to the edge improves latency for time-sensitive traffic.

Local breakout: enterprises and venues can run their applications and store their content locally and can use their small-cell infrastructure to deliver their own services in addition to operator and over-the-top (OTT) services.

Enterprise/venue-funded: the enterprise or venue can time, size and plan the IBW network to meet its own requirements and funding availability. It can also control network operations and usage, either directly or, more likely, through a neutral host or other third party.

More control for the enterprise, less effort for carriers: the enterprise/venue pays for the infrastructure it needs, while the carrier provides the connectivity and integration to the wide-area network.

Stronger security: the local edge-computing infrastructure decreases the vulnerability to network-wide attacks.

Integration with enterprise and venue Wi-Fi: Wi-Fi will continue to provide most connectivity through a strong and cost-effective ecosystem, but Wi-Fi and small cells can both improve performance when integrated.

Support for IoT and Industrial IoT (IIoT): indoor small cells can support enterprise or venue-based IoT or IIoT applications in private networks that are not part of a mobile network.

IBW has become crucial for many entities that control real estate: some need the functionality it provides to run location-based services and basic connectivity, others see it as an amenity that increases the value of their real estate – and many of them want both.

In parallel, new small-cell solutions and edge-computing capabilities enable and strengthen the business model evolution, by facilitating the involvement of the enterprise and venue owners.

Small-cell equipment is increasingly designed to support sharing between the venue owner/enterprise and multiple operators – often with the mediation of a neutral host, which may plan, deploy and operate a network and establish relations among the involved parties. In-building deployments of this new generation of small cells make it possible to support multiple frequencies (including unlicensed access), combine multiple cells or sectors in the same enclosure, share backhaul, have centralized architectures, and use Ethernet for backhaul. Crucially, in this deployment model, operators can participate in a multi-operator IBW network, but retain exclusive use of their spectrum assets, as they currently do with distributed antenna systems (DAS).

Private LTE networks that venue owners and enterprises can deploy independently of mobile operators have started to gain great traction in the enterprise today. With 5G, private networks adoption will grow, and they will support additional functionality. Private networks can support a wide range of services that are local to the enterprise and that may have specific requirements – for instance, for reliability, latency, or security – but they can be operated with stripped-down, less complex core functionality.

In the US, the introduction of spectrum sharing in the 3.5 GHz Citizens Broadband Radio Service (CBRS) band using OnGo creates a major incentive for enterprises to deploy private networks, with up to 150 MHz of clean spectrum without having to purchase a license.

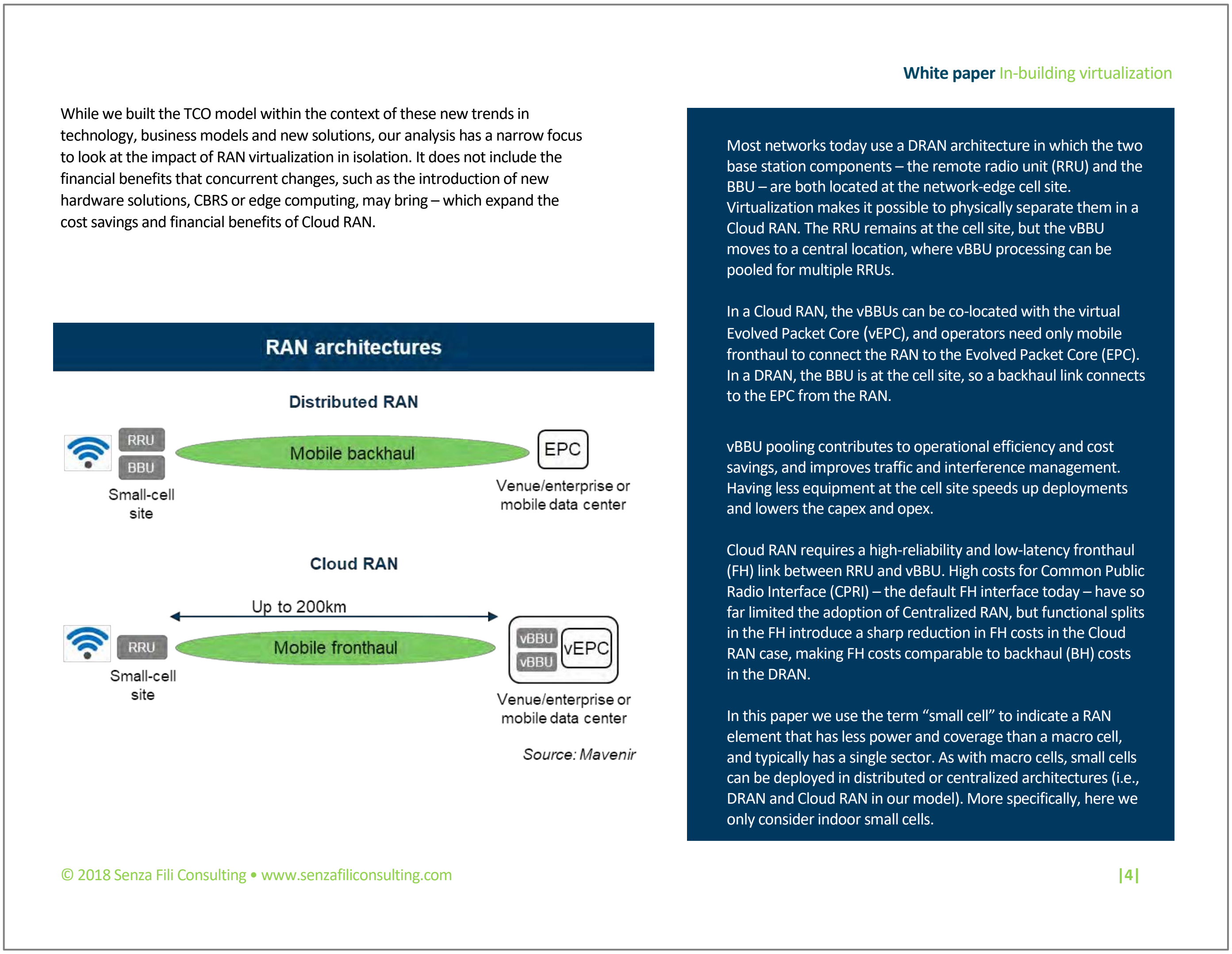
At an end-to-end network level, virtualization in the RAN and in the core provides the flexibility that operators and the enterprise/venue owners need to establish a deeper collaboration framework that is mutually advantageous and that delivers improved network and financial efficiency.

With virtualization in the RAN with Cloud RAN, small cells can use a split architecture, in which the remote radio unit (RRU) sits at locations of high traffic inside buildings, and a virtual BBU (vBBU) is located within a remote location, either physically within the venue or in the cloud. The first option may appeal to venues that are larger or have demanding requirements. The second option may be more attractive to mid-size and small venues that would find it too complex and expensive to host dedicated BBUs.

Core virtualization is a great enabler for moving functionality to the edge. For the enterprise and venue owners, this greatly expands the ability to deploy and control services and functionality that is local to them, and over which they have full access and control, if they need it.

Edge computing and RAN virtualization are complementary and mutually reinforcing, because the vBBUs can be co-located with the edge infrastructure. Not only does this help reduce the costs, but it also improves the performance benefits of both as traffic management and resource optimization can be jointly performed at the edge/vBBU location.

This paper is a companion to two previous papers. The first white paper, "How much can operators save with a Cloud RAN? A total cost of ownership (TCO) model for virtualized and distributed RAN," compares the TCO for distributed RAN (DRAN) and Cloud RAN. The second white paper, "Future proofing mobile networks economics. Accessing the TCO for Cloud RAN and Centralized RAN," looks at two remote-BBU topologies – Centralized RAN and Cloud RAN – using the same TCO model we use here, and we then compare them to the DRAN TCO.



While we built the TCO model within the context of these new trends in technology, business models and new solutions, our analysis has a narrow focus to look at the impact of RAN virtualization in isolation. It does not include the financial benefits that concurrent changes, such as the introduction of new hardware solutions, CBRS or edge computing, may bring – which expand the cost savings and financial benefits of Cloud RAN.

RAN architectures

Source: Mavenir

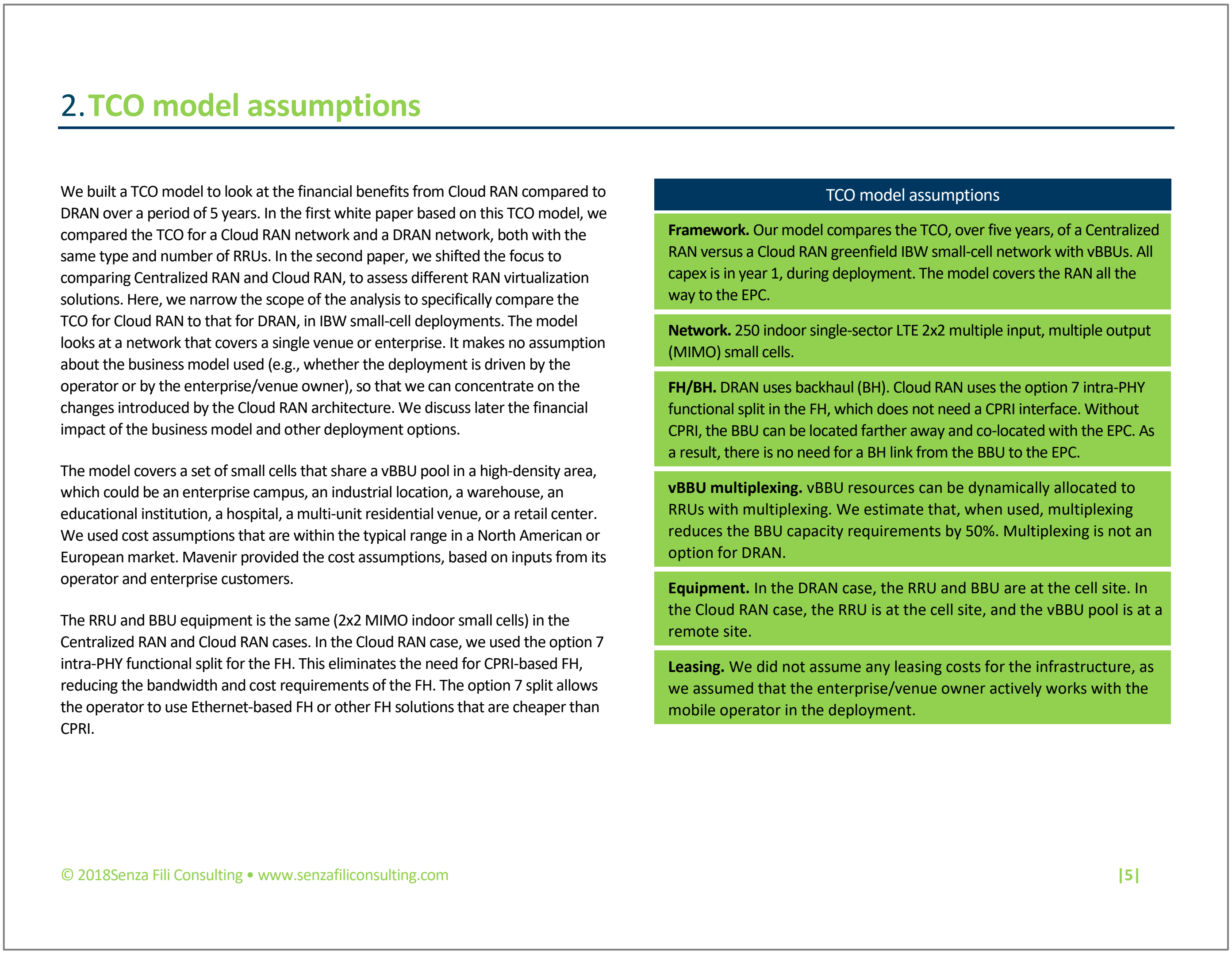
Most networks today use a DRAN architecture in which the two base station components – the remote radio unit (RRU) and the BBU – are both located at the network-edge cell site. Virtualization makes it possible to physically separate them in a Cloud RAN. The RRU remains at the cell site, but the vBBU moves to a central location, where vBBU processing can be pooled for multiple RRUs.

In a Cloud RAN, the vBBUs can be co-located with the virtual Evolved Packet Core (vEPC), and operators need only mobile fronthaul to connect the RAN to the Evolved Packet Core (EPC). In a DRAN, the BBU is at the cell site, so a backhaul link connects to the EPC from the RAN.

vBBU pooling contributes to operational efficiency and cost savings, and improves traffic and interference management. Having less equipment at the cell site speeds up deployments and lowers the capex and opex.

Cloud RAN requires a high-reliability and low-latency fronthaul (FH) link between RRU and vBBU. High costs for Common Public Radio Interface (CPRI) – the default FH interface today – have so far limited the adoption of Centralized RAN, but functional splits in the FH introduce a sharp reduction in FH costs in the Cloud RAN case, making FH costs comparable to backhaul (BH) costs in the DRAN.

In this paper we use the term "small cell" to indicate a RAN element that has less power and coverage than a macro cell, and typically has a single sector. As with macro cells, small cells can be deployed in distributed or centralized architectures (i.e., DRAN and Cloud RAN in our model). More specifically, here we only consider indoor small cells.



2. TCO model assumptions

We built a TCO model to look at the financial benefits from Cloud RAN compared to DRAN over a period of 5 years. In the first white paper based on this TCO model, we compared the TCO for a Cloud RAN network and a DRAN network, both with the same type and number of RRUs. In the second paper, we shifted the focus to comparing Centralized RAN and Cloud RAN, to assess different RAN virtualization solutions. Here, we narrow the scope of the analysis to specifically compare the TCO for Cloud RAN to that for DRAN, in IBW small-cell deployments. The model looks at a network that covers a single venue or enterprise. It makes no assumption about the business model used (e.g., whether the deployment is driven by the operator or by the enterprise/venue owner), so that we can concentrate on the changes introduced by the Cloud RAN architecture. We discuss later the financial impact of the business model and other deployment options.

The model covers a set of small cells that share a vBBU pool in a high-density area, which could be an enterprise campus, an industrial location, a warehouse, an educational institution, a hospital, a multi-unit residential venue, or a retail center. We used cost assumptions that are within the typical range in a North American or European market. Mavenir provided the cost assumptions, based on inputs from its operator and enterprise customers.

The RRU and BBU equipment is the same (2x2 MIMO indoor small cells) in the Centralized RAN and Cloud RAN cases. In the Cloud RAN case, we used the option 7 intra-PHY functional split for the FH. This eliminates the need for CPRI-based FH, reducing the bandwidth and cost requirements of the FH. The option 7 split allows the operator to use Ethernet-based FH or other FH solutions that are cheaper than CPRI.

TCO model assumptions

Framework. Our model compares the TCO, over five years, of a Centralized RAN versus a Cloud RAN greenfield IBW small-cell network with vBBUs. All capex is in year 1, during deployment. The model covers the RAN all the way to the EPC.

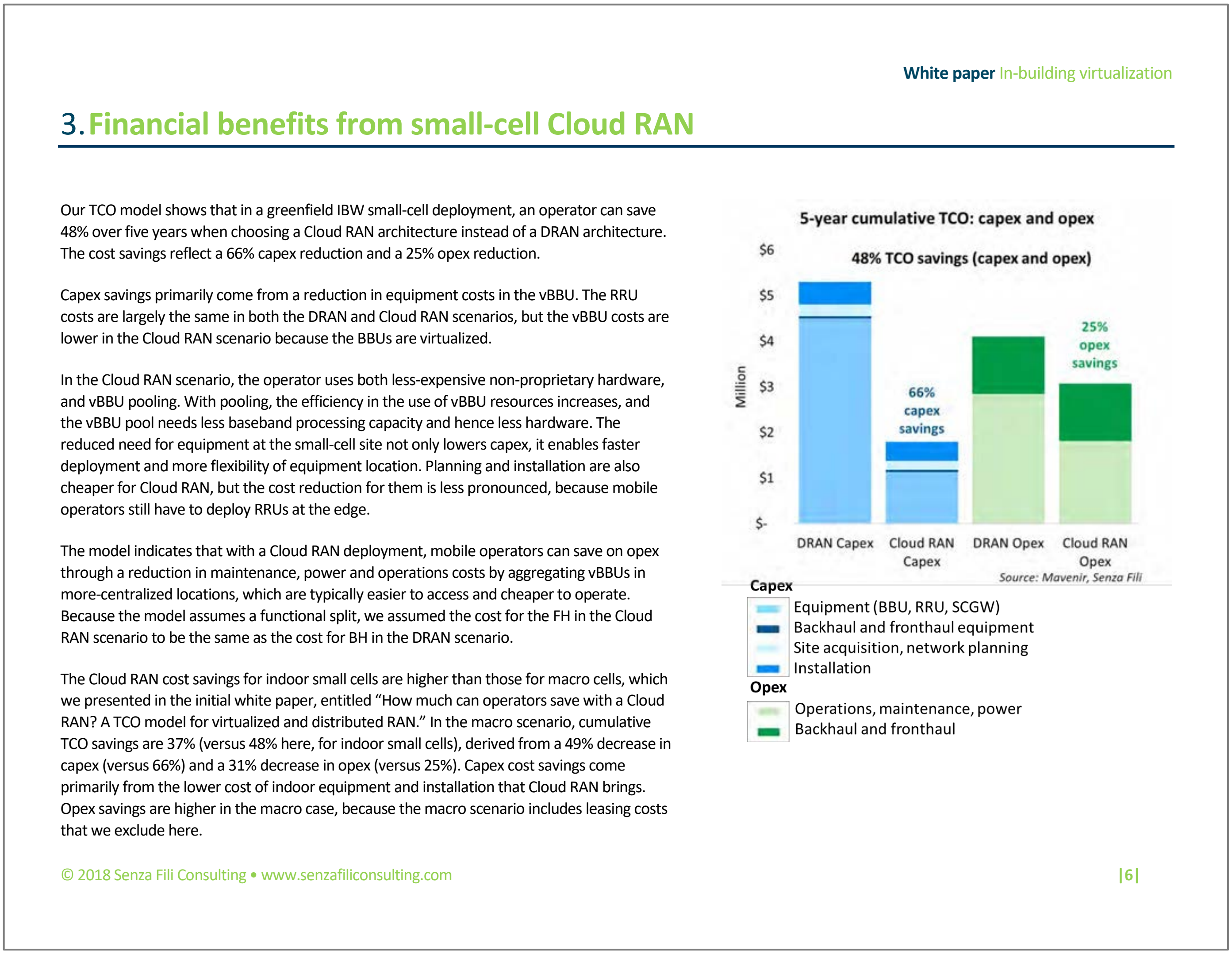
Network. 250 indoor single-sector LTE 2x2 multiple input, multiple output (MIMO) small cells.

FH/BH. DRAN uses backhaul (BH). Cloud RAN uses the option 7 intra-PHY functional split in the FH, which does not need a CPRI interface. Without CPRI, the BBU can be located farther away and co-located with the EPC. As a result, there is no need for a BH link from the BBU to the EPC.

vBBU multiplexing. vBBU resources can be dynamically allocated to RRUs with multiplexing. We estimate that, when used, multiplexing reduces the BBU capacity requirements by 50%. Multiplexing is not an option for DRAN.

Equipment. In the DRAN case, the RRU and BBU are at the cell site. In the Cloud RAN case, the RRU is at the cell site, and the vBBU pool is at a remote site.

Leasing. We did not assume any leasing costs for the infrastructure, as we assumed that the enterprise/venue owner actively works with the mobile operator in the deployment.



3. Financial benefits from small-cell Cloud RAN

Our TCO model shows that in a greenfield IBW small-cell deployment, an operator can save 48% over five years when choosing a Cloud RAN architecture instead of a DRAN architecture. The cost savings reflect a 66% capex reduction and a 25% opex reduction.

Capex savings primarily come from a reduction in equipment costs in the vBBU. The RRU costs are largely the same in both the DRAN and Cloud RAN scenarios, but the vBBU costs are lower in the Cloud RAN scenario because the BBUs are virtualized.

In the Cloud RAN scenario, the operator uses both less-expensive non-proprietary hardware, and vBBU pooling. With pooling, the efficiency in the use of vBBU resources increases, and the vBBU pool needs less baseband processing capacity and hence less hardware. The reduced need for equipment at the small-cell site not only lowers capex, it enables faster deployment and more flexibility of equipment location. Planning and installation are also cheaper for Cloud RAN, but the cost reduction for them is less pronounced, because mobile operators still have to deploy RRUs at the edge.

The model indicates that with a Cloud RAN deployment, mobile operators can save on opex through a reduction in maintenance, power and operations costs by aggregating vBBUs in more-centralized locations, which are typically easier to access and cheaper to operate. Because the model assumes a functional split, we assumed the cost for the FH in the Cloud RAN scenario to be the same as the cost for BH in the DRAN scenario.

The Cloud RAN cost savings for indoor small cells are higher than those for macro cells, which we presented in the initial white paper, entitled “How much can operators save with a Cloud RAN? A TCO model for virtualized and distributed RAN.” In the macro scenario, cumulative TCO savings are 37% (versus 48% here, for indoor small cells), derived from a 49% decrease in capex (versus 66%) and a 31% decrease in opex (versus 25%). Capex cost savings come primarily from the lower cost of indoor equipment and installation that Cloud RAN brings. Opex savings are higher in the macro case, because the macro scenario includes leasing costs that we exclude here.

5-year cumulative TCO: capex and opex

48% TCO savings (capex and opex)

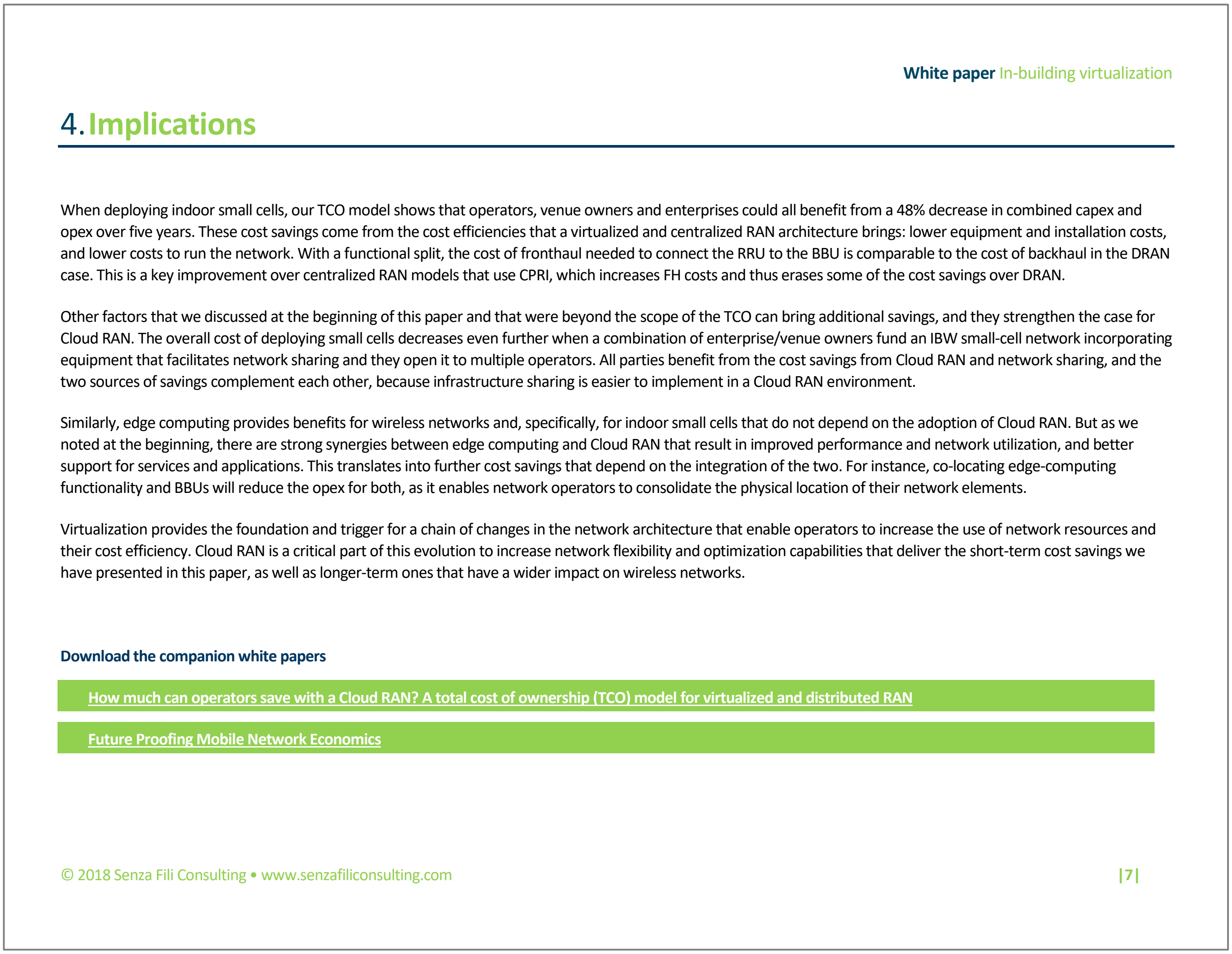
Source: Mavenir, Senza Fili

Capex

- 🟦 Equipment (BBU, RRU, SCGW)
- 🟦 Backhaul and fronthaul equipment
- 🟦 Site acquisition, network planning
- 🟦 Installation

Opex

- 🟩 Operations, maintenance, power
- 🟩 Backhaul and fronthaul



4. Implications

When deploying indoor small cells, our TCO model shows that operators, venue owners and enterprises could all benefit from a 48% decrease in combined capex and opex over five years. These cost savings come from the cost efficiencies that a virtualized and centralized RAN architecture brings: lower equipment and installation costs, and lower costs to run the network. With a functional split, the cost of fronthaul needed to connect the RRU to the BBU is comparable to the cost of backhaul in the DRAN case. This is a key improvement over centralized RAN models that use CPRI, which increases FH costs and thus erases some of the cost savings over DRAN.

Other factors that we discussed at the beginning of this paper and that were beyond the scope of the TCO can bring additional savings, and they strengthen the case for Cloud RAN. The overall cost of deploying small cells decreases even further when a combination of enterprise/venue owners fund an IBW small-cell network incorporating equipment that facilitates network sharing and they open it to multiple operators. All parties benefit from the cost savings from Cloud RAN and network sharing, and the two sources of savings complement each other, because infrastructure sharing is easier to implement in a Cloud RAN environment.

Similarly, edge computing provides benefits for wireless networks and, specifically, for indoor small cells that do not depend on the adoption of Cloud RAN. But as we noted at the beginning, there are strong synergies between edge computing and Cloud RAN that result in improved performance and network utilization, and better support for services and applications. This translates into further cost savings that depend on the integration of the two. For instance, co-locating edge-computing functionality and BBUs will reduce the opex for both, as it enables network operators to consolidate the physical location of their network elements.

Virtualization provides the foundation and trigger for a chain of changes in the network architecture that enable operators to increase the use of network resources and their cost efficiency. Cloud RAN is a critical part of this evolution to increase network flexibility and optimization capabilities that deliver the short-term cost savings we have presented in this paper, as well as longer-term ones that have a wider impact on wireless networks.

Download the companion white papers

How much can operators save with a Cloud RAN? A total cost of ownership (TCO) model for virtualized and distributed RAN

Future Proofing Mobile Network Economics

About Mavenir

Mavenir is the industry’s only end-to-end, cloud-native network software provider, redefining network economics for Communication Service Providers (CSPs). Our innovative solutions pave the way to 5G with 100% software-based, end-to-end, cloud-native network solutions. Leveraging industry-leading firsts in VoLTE, VoWiFi, Advanced Messaging (RCS), Multi-ID, vEPC and vRAN, Mavenir accelerates network transformation for 250+ CSP customers in over 130 countries, serving over 50% of the world’s subscribers. We embrace disruptive, innovative technology architectures and business models that drive service agility, flexibility, and velocity. With solutions that propel NFV evolution to achieve web-scale economics, Mavenir offers solutions to CSPs for revenue generation, cost reduction and revenue protection.

For more information, please visit our website at www.mavenir.com